Anno 2 - N. 24
24 Aprile - 8 Maggio 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it,

Contributors: boymix81, CAT4R4TTA, Roberto "decOder" Enea, Nicola D'Agostino, lele@altos.tk, {RoSwElL}, Paola Tigrino, 3d0

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Immagine di copertina: Zocdesign.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack'er (hãk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

PAURA E DELIRIO A LOS WINDOWS

Non so come e perché mi trovo qui, ma sono davanti a un computer, e ho bisogno di usarlo. All'avvio, una finestrella mi avverte che devo scaricare un importante aggiornamento. Le dico di ripassare più tardi, perché adesso ho da fare, e quella si ripresenta più o meno ogni minuto. Decido di seguire il suggerimento/obbligo all'aggiornamento.

Improvvisamente, compare un'altra finestra sullo schermo: Nicole vuole invitarmi sul suo sito. Nicole mi ha sparato un messaggio automatico superando le deboli difese del programma di messaggistica che non ho scelto di installare, che ho chiesto di rimuovere, ma che ogni aggiornamento di sistema ripristina nella sua versione più recente, e attiva all'avvio.

Intanto, cerco l'icona del programma che mi serve tra una cinquantina di icone che ogni programma installato ha piazzato sul Desktop. Trovo il programma giusto; è più o meno al centro dello schermo. Ci faccio doppio clic. Improvvisamente arriva il quarto messaggio di Nicole, proprio mentre il mouse è al centro dello schermo, e il clic finisce proprio sul link del sito di Nicole. Mi incazzo, e pesto i pugni sul tavolo. Il mouse cade giù dalla scrivania, e Switch gli salta addosso per giocarci (può un gatto resistere dall'assaltare un topo?). Ovviamente, mentre io cerco di ripescare il mouse, Switch preme un paio di pulsanti, che finiscono col farmi scaricare e installare un dialer (anche se la finestra che vedo sullo schermo dice solo "Aggiornamento multimediale"). Il dialer mi collega a qualche centrale telefonica cilena, o di qualche posto lontano e costosissimo. Preso dal panico, strappo la linea telefonica dal muro, e cerco di chiudere la finestra del sito di Nicole, ma se ne apre un'altra, e poi un'altra ancora, e altre sullo sfondo: Samantha con l'acca, Samanta senza acca, Suzy, Tatiana... finestre ovunque, e più ne chiudo e più se ne aprono. Riavvio il computer, ma quando riparte il sistema, ripartono le finestre. Respiro in modo affannato, poi mi aggrappo a un raggio di luce e, finalmente, mi sveglio.

Sono sudato fradicio, nel mio letto. Riprendo fiato. Mi sollevo. Era un incubo. Del resto, un sistema operativo che consenta simili porcherie non esiste, giusto?

Faccio due passi e, per prendere una boccata d'aria fresca, apro la finestra e mi affaccio. Di colpo, tutte le finestre dei palazzi vicini si aprono una dopo l'altra. Nella via riecheggia il mio urlo...

grand@hackerjournal.it

www.hackerjournal.it

Saremo di nuovo in edicola Giovedì 8 maggio!

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

CHIAREZZA SULLA SECRET ZONE

La Secret Zone è l'area riservata del nostro sito in cui si trovano gli arretrati in formato Pdf, il modulo per registrare un'email gratuita con indirizzo @hackerjournal.it la possibilità di acquistare libri Hops con lo sconto del 15%, alcuni loghi per cellulari gratuiti e alcuni altri "servizi riservati".

Per accedere alla Secret Zone si utilizzano i codici che si trovano in questa pagina, e che sono diversi per ogni numero di HJ; questi sono validi solo finché il numero corrente rimane in edicola.

Questo significa che le password che si trovano su Hacker Journal Collection (la raccolta degli arretrati), non valgono più. Fate attenzione anche a non confondere lettere e numeri: i codici possono sempre essere letti come parole di senso compiuto (in questo numero, "bussolotto" ed "equestre"). Occhio quindi a non confondere 1 (uno) con l (elle), o 0 (zero) con O.

I NOSTRI/VOSTRI BANNER!

Nel momento in cui scriviamo, siamo arrivati a ben 88 banner realizzati da voi e pubblicati sul sito di HJ. Ecco i più belli di questo numero:

Zerothenewhack

Neuromante

Simonetta

Klaus74

Maga84

Dai bit alla carta

http://web.tiscali.it/juniord2003

http://www.blood-hacker.tk/

http://digilander.libero.it/indyjour/

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: bussol8
pass: eques3

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

mailto:

redazione@hackerjournal.it

TESCHI E PIRATI

Nei vostri articoli parlate sempre del fatto che gli hacker non vanno criminalizzati, che sono semplicemente degli appassionati di tecnologia e (citando Mentor), il loro unico crimine è la curiosità. Poi però le vostre copertine sono piene di teschi. Perché?

Il mondo degli hacker e il jolly roger, la bandiera dei pirati, sono legati da quasi trent'anni. Nell'ufficio del team che ha progettato il Macintosh, sventolava la bandiera nera col teschio e le tibie (tanto che un recente film su quelle vicende si chiama proprio "Pirates of Silicon Valley"); una famosa foto che circolava sui BBS molto prima dell'Internet commerciale, mostrava la famigerata bandiera che sventolava dalla sede della AT&T (la vedete qui accanto). E non solo: riviste ciclostilate o elettroniche, BBS prima e siti Web poi, hanno spesso fatto uso di questo simbolo nel contesto dell'hacking.
Il motivo per cui l'abbiamo scelta come logo (e per cui quindi è diventato un elemento grafico ricorsivo), è un po' per prendere in giro i media tradizionali, sempre pronti a criminalizzare chiunque, e un po' noi stessi e il nostro mondo. E poi, tra amici con affinità simili, si può scherzare sopra agli elementi comuni (le più pesanti battute sui gay, le ho sentite proprio da amici omosessuali). Ma qualcuno ci ha preso davvero sul serio quando abbiamo ritratto uno scheletro nei panni della Gioconda? Relax, gente...

☺ Tech Humor ☺

Non sperate di riuscire a riconfigurare meglio XFree86 dopo aver bevuto tre o quattro bottiglie di birra Hacker.

QUALITÀ DEL SOFTWARE LIBERO

Volevo porvi una domanda che spero pubblichiate anke sulla rivista perché penso che in molti se la siano posta ma senza risposta: in questi tempi sempre di più si parla di software libero e che questo molto probabilmente si affermerà sempre più in futuro. Ma io mi chiedo, di che qualità sarà questo software? Sarà scritto solo da programmatori che per hobby e per bontà ce lo metteranno a disposizione? Chi sono i programmatori che per hobby si mettono a scrivere magari un CAD di qualità per un\'azienda? Già ora ci lamentiamo che gran parte del software libero gira solo in inglese perché nessuno si sbatte per tradurlo… figuriamoci in futuro!!! Da parte mia e di altre persone spero proprio che possiate fornirci chiarimenti, e chi meglio di voi!!!

Khann

E chi l'avrebbe mai detto che qualcuno si mettesse a sviluppare un sistema operativo libero, dal kernel agli applicativi di ufficio? Eppure c'è (anzi, ce n'è più d'uno...). Io credo che nessuno abbia il diritto di "lamentarsi" se non esiste un software libero che fa per lui, o se non c'è nella sua lingua. L'approccio corretto sarebbe quello di contribuire alla realizzazione del software che ti interessa. Nel caso delle società, per esempio assumendo un programmatore, o finanziando una comunità di sviluppo già esistente, perché apporti al software libero le modifiche che le interessano. Modifiche che poi, ovviamente, andranno rese disponibili al pubblico secondo la stessa licenza.

LINUX SU PC VECCHI

Ho recuperato un vecchio computer con Pentium 233 e 16 Mbyte di RAM. Avendo sentito che Linux funziona bene anche su macchine molto lente, mi ero convinto a provare a installarlo. Leggendo in giro i requisiti minimi della varie distribuzioni, e sentendo i pareri di altri che hanno già montato Linux, pare che ci voglia almeno un Pentium II con 64 o 128 Mbyte di RAM. Ma allora, Linux è esoso di risorse quanto e più di Windows?

Ktm

Quando si dice che Linux funziona egregiamente anche su macchine lente e con poca memoria, spesso ci si riferisce (senza dirlo esplicitamente) alle sue qualità di server. Se lo avvii a linea di comando, puoi farci girare un server Web, ftp e tenere loggati svariati utenti senza che faccia una piega.
Quando invece lo si vuole usare come normale stazione di lavoro, con interfaccia grafica, i requisiti salgono drasticamente, soprattutto in termini di memoria RAM (usare una versione recente di XFree86 con meno di 64 MByte di memoria è quasi impensabile).
Se comunque intendi usare Linux per

riportare in vita il vecchio computer, e utilizzarlo per compiti piuttosto semplici (niente fotoritocco o Quake...), puoi provare VectorLinux (www.vectorlinux.com), una distribuzione pensata soprattutto per i casi come il tuo. Oltre alla versione più recente di XFree86, comprende infatti anche la versione 3.3.6. Io l'ho installato su un notebook Pentium 150 con 16 Mbyte di RAM, e ci si riesce a scrivere con AbiWord, navigare con Opera (aspettando un po' il disegno delle pagine...), leggere la posta e svolgere compiti quotidiani.

LEGALITÀ DEI DIVX

Se si compra la qualsiasi delle riviste informatiche anke quelle per principianti (che mi fanno ridere per quello che dicono, con tutto il rispetto per i principianti), ci si imbatte quasi sicuramente in articoli ke parlano di divx: cosa sono, come si fanno, perché si fanno (backup, assolutamente backup). Mi sono però stupito quando ho letto questo: "dove si trovano e come si prendono". Leggo bene? Stai suggerendo come scaricarti film, anke quelli non ancora usciti nei cinema di tutto il mondo? Stai insomma istigando alla pirateria (parliamo kiaro)?
Ebbene, ho letto articoli di questo genere, che spiegano passo passo dallo scaricare ed installre un programma di file sharing fino al download per arrivare agli strumenti necessari per riprodurli e masterizzarli (ovviamente il più furbo dei lettori aggiunge anche la vendita a tutto il processo).
Proprio in una rivista per principianti c'è un articolo che spiega tutto. Tutto tranne il fatto che si può incorrere in multe e galera. Lo sporvveduto ke legge l'articolo non si pone problemi, specialmente se ha adsl. L'articolo arriva in conclusione con una frase del genere "Insomma, chi ha voglia di cinema può sfruttare, una volta di più e in modo legale, la rete". Legale?
Come disclaimer dice solo "chi vuol fare il furbo trova, cmq, molto materiale da usare a proprio rischio e pericolo, visto che si tratta di un'operazione vietata". "Vietata" ma "Legale". So benissimo che tra "vietato" e "illegale" non c'è molta differenza, però ILLEGALE suona meglio di VIETATA.

Th3_Sl33P

E poi se la prendono con noi per qualche teschio ;-)
In ogni caso, per dovere di cronaca segnaliamo che il semplice possesso di musica o video copiati non è un reato penale; il titolare dei diritti può semplicemente chiedere la distruzione delle copie e il risarcimento del danno (il prezzo del disco o del film). È invece un reato di tipo penale la vendita di copie illegali. Per quanto riguarda il software, invece, la situazione è diversa: anche il semplice possesso o utilizzo a fini non di lucro può essere considerato reato.

IL BANNER DI HJ

Salve, potreste mandarmi il vostro banner da inserire nel mio sito visto che è stato pubblicato qualche tempo fa su Hacker Journal?

Ne trovi a dozzine su http://www.hackerjournal.it/php-bin/gof.php?go=artworks
Scegli quello che preferisci!

DIALER E ADSL

Gentile Redazione, volevo sapere se con una connessione ADSL È possibile che un dialer possa giocare gli stessi scherzi che gioca alle normali connessioni.

Marco S.

No, a meno che tu non abbia anche un modem collegato alla linea telefonica, non è possibile che il dialer ti colleghi a numeri a pagamento. In ogni caso, è bene prevenire il problema alla fonte, evitando l'esecuzione di codici e programmi non autorizzati sul proprio computer. Meglio innalzare le difese, perché non sai mai cosa può esserci nascosto in un piccolo .exe.

MOLESTIE VIA SMS

Vi pregherei gentilmente di indicarmi se esistono siti o programmi che possano aiutarmi a risalire alla localizzazione (anche solo parziale, meglio se totale), noto l'IP di un computer collegato. Trattasi di un maleducato che importuna una mia collega con frasi oscene, mandando sms tramite www.enel.it. Ho quindi a disposizione l'IP (che ENEL invia) del mittente.

Ing. Massimo A.

Sì, per esempio puoi usare il comando tracert su Windows (da Start/Esegui inserisci tracert _indirizzo_ip_). Però, se il maleducato ha coperto le sue tracce, rischi di arrivare a un proxy o a un utente ignaro di tutto.
In questo caso, puoi provare a segnalare la cosa a Enel.it o - nei casi più gravi - rivolgerti all'Autorità Giudiziaria, l'unica che abbia il potere di recuperare l'informazione completa del mittente dei messaggi. Anche dopo aver trovato il suo indirizzo IP, infatti, non potresti comunque risalire all'identità della persona, se questa si collega da casa con un modem. Le forze dell'Ordine invece possono richiedere questo dato al provider. Se decidi di fare questa scelta, tieni presente che la conseguenza potrebbe essere un processo.

☺ Tech Humor ☺

Sopresi di vedere un utente Linux così giovane? Beh, sapendo che Alice di congome fa Tovalds, e che il suo papà si chiama Linux, si spiegano molte cose.

NEWS

HOT!

UN PRESARIO A 319 DOLLARI

Costa meno di 300 euro il Compaq Presario S3000V, con processore Celeron da 2 Gigahertz, 128 MB di RAM, un disco da 40 GB e un lettore di CD-ROM. HP ha iniziato a venderlo negli Stati Uniti battendo il record del PC più economico nella sua categoria. Nel caso ci fossero dei dubbi, non rende molto con Unreal e il monitor è a parte.

FRODI IN RETE

Sono triplicate, secondo l'FBI, le frodi commesse in Rete nel 2002.
Aziende che mettono all'asta prodotti e poi fanno offerte fasulle per alzare il prezzo, articoli ordinati, pagati e mai consegnati e addebiti a casaccio sulle carte di credito sono i problemi segnalati più di frequente allo IFCC, l'ufficio federale contro le truffe via Internet.
Ad alzare un bel po' il numero delle segnalazioni per il 2002 è stato il gran numero di persone che si sono lasciate imbrogliare dalla fantomatica email dei ricchi nigeriani che vorrebbero depiositare qualche miliardo sul tuo conto corrente ma prima devi pagare qualcosina per le spese.

PAKISTAN INTERNET 1 A 0

Se qualcuno pensava che i problemi dei pakistani riguardassero cose come mangiare, bere, evitare gli scontri a fuoco e proteggersi dal freddo sappia che si sbagliava: il vero problema è Internet e, nello specifico, i siti pornografici, quelli anti islamici e quelli blasfemi. Appena trova un sito del genere, il governo ne blocca l'accesso da qualsiasi connessione attiva nel Paese. Lode allo sforzo ciclopico della commissione deputata alla censura.

100 E NON PIÙ DI 100

Dopo aver constatato che una parte spaventosamente consistente del traffico sui suoi server è costituito da spam, Hotmail ha deciso di limitare a cento il numero massimo di messaggi che ciascun account può inviare. La lotta dei vari provider e di Microsoft contro lo spam è iniziata da un pezzo e ha avuto alti e bassi. In un estremo tentativo di limitare il traffico, per esempio, l'azienda di Redmond ha creato una "lista nera" di spammers i cui messaggi non potranno mai raggiungere uno qualsiasi dei 120 milioni di indirizzi Hotmail. Peccato davvero che, per alcuni giorni, su questa lista ci sono finiti nientemeno che RoadRunner, provider di AOL Time Warner, e EarthLink, altro network di primo piano negli USA. Per alcuni giorni, in pratica, nessun abbonato a questi due servizi ha potuto spedire messaggi a indirizzi MSN. Come già AOL e Earthlink, anche Microsoft si appresta a far causa a un buon numero di spammers. La vittoria legale è quasi certa e i soldi arrivano subito. Chi volesse provare a combattere gli spammer da solo sappia che ha ottime possibilità di farcela, basta conservare le mail non richieste e ricorrere al Garante per la Privacy per tirar su soldi a sufficienza per offrire una cena agli amici. Se non ci credete, date un'occhiata su http://www.maxkava.com/spam/.

Sempre a proposito di privacy, Microsoft ha disattivato ufficialmente un servizio da sempre piuttosto ambiguo: il portafogli elettronico di Passport per gli acquisti su Internet. La società di Redmond ha deciso, chiaramente per conto suo, di cancellare anche tutti i dati sulle carte di credito inseriti dai sempre fiduciosi utenti del suo servizio. Chissà perché.

DOPO LE PECORE, SI CLONANO LE MELE

Chi si ricorda i cosiddetti "cloni" Mac di qualche anno fa, cioè computer che usavano il sistema operativo di Apple ma che erano costruiti da altre aziende, forse storcerà il naso, ma la situazione è diversa. Stavolta Apple non ha dato nessuna licenza, e la macchina che il ventunenne John Fraser sta finendo di realizzare verrà venduta senza sistema operativo e creata con parti di ricambio di G4. L'obiettivo è offrire un Mac al prezzo di un PC economico, ma la lotta non sembra facile. Primo perché iBox assomiglia più a un cartone per la pizza che a un Mac, secondo perché nessuno dentro a Apple ha ancora confermato che l'azienda di Cupertino non scatenerà contro il giovane Fraser le sue orde assatanate di legali. Staremo a vedere, intanto date un'occhiata alla meraviglia che ci aspetta, ma non fatevi venire strane idee: non si mangia.

UN NOKIA CHE SOMIGLIA A UN GAMEBOY

In occasione del Cebit, Nokia ha presentato una serie di nuovi cellulari.
Nokia 810 è un telefono veicolare, con vivavoce e antenna esterna, supporto Bluetooth, GPRS e HSCSD. Dotato di una ruota di navigazione studiata per l'utilizzo in auto, è nato per rendere semplice, veloce e sicura la comunicazione vocale e lo scambio di dati durante gli spostamenti. Lo schermo retroilluminato è separato dal telefono e posizionabile a scelta. La memoria può essere utilizzata separatamente da due utenti. C'è anche un terminale GSM che si collega a un centralino telefonico per gestire chiamate GSM 850/1900 o GSM 900/1800 ed è perfetto per allestire una rete di linee mobili in ufficio. Il Nokia 3300 è utilizzabile, oltre che come cellulare, anche come lettore MP3, radio FM stereo e registratore digitale. Assomiglia a un Gameboy ma non siamo ancora riusciti a giocarci in maniera decente. Supporta le Multimedia Card, e con la funzione True Tones, possiamo usare qualsiasi suono come suoneria. Il Nokia 6220 è uno smartphone destinato alla gente in movimento. E' dotato di display a colori, personal organizer, tribanda e velocità dati pari a 118,4 kbps, di gran lunga più veloce del tradizionale Gprs, e di una fotocamera digitale integrata che consente di catturare immagini ed inviare messaggi MMS.
L'ultimo gioiello presentato da Nokia, invece, non è un telefono ma un accessorio assolutamente unico: la Nokia Digital Pen, che permette di scrivere o disegnare a mano libera su un particolare tipo di carta, ed inviare poi il tutto a un cellulare compatibile mediante Bluetooth.

FACCIAMOLO SU DVD

Adobe sta per lanciare sul mercato EncoreDVD, un nuovo pacchetto software dedicato all'authoring professionale di Dvd, per lavorare, in qualsiasi formato Dvd registrabile, sul video e aggiungere menu, sottotitoli e altri contenuti. EncoreDVD, secondo Adobe, costituisce finalmente un'offerta completa, dopo le applicazioni con funzionalità di base allegate a Premiere e ad altri prodotti simili.
La caratteristica più importante di questo pacchetto è senza dubbio la completa integrazione con Photoshop, Premiere e After Effects, che permette di operare sui contenuti multimediali mediante questi sofisticati strumenti e ottenere anche menu interattivi e filmati multilingua. E' possibile inoltre convertire i filmati in formato Mpeg-2 e le tracce audio in formato Dolby Digital. Il prezzo previsto sarà di circa 550 dollari, e, fatto piuttosto sconcertante per gli standard Adobe, non è prevista una versione Mac, forse perché Macintosh già dispone di un popolare pacchetto di Dvd authoring, Dvd Pro.

CASA BIANCA DEFACCIATA

Non si fermano davanti a nulla i cracker che vogliono protestare, a modo loro, contro l'intervento statunitense in Iraq. Il sito della Casa Bianca avrebbe subito un, seppur breve, defacement: sulla home page appariva soltanto una frase che si interrogava sul perché della guerra, a firma "Owned by Free World". Dall'altra parte dell'oceano, invece, il sito del Governo britannico ha subito un attacco DOS, che lo ha reso irraggiungibile per parecchie ore.

BUFALA DI GUERRA

Sta girando in Rete, ormai da parecchio tempo, un documento Powerpoint intitolato "Perché si fa una guerra", impropriamente associato all'associazione umanitaria Emergency, in quanto nel finale fa riferimento a un appello a cura dell'associazione stessa. Emergency ha quindi pubblicato sul proprio sito una comunicazione, smentendo la paternità del documento e precisando che si tratta di dati raccolti in maniera un po' sommaria da uno studente durante una lezione universitaria.

NUOVO VIRUS: HAWAWI

E' un worm, segnalato a livello di pericolosità 2, distribuito via email, ma anche attraverso i sistemi di file sharing come Kazaa e WinMX, nonché mediante i più popolari messenger. A differenza degli worm per file sharing già noti, che si limitano a creare traffico inutile, Hawawi sovrascrive i file con le estensioni più comuni, cancellandone il contenuto. A rischio sono eseguibili e archivi, ma anche immagini, documenti e pagine Web.

NEWS

HOT!

VIDEOSCUOLA IN OSPEDALE

Il Ministero dell'Istruzione ha recentemente presentato un progetto per integrare e rendere più efficace il già esistente servizio Scuola in Ospedale, volto all'assistenza di bambini e adolescenti che devono trascorrere molto tempo in un luogo di cura e desiderano restare alla pari con i loro corsi di studio. I corsi di sostegno saranno supportati da un servizio estremamente avanzato con funzioni di videoconferenza, in modo che gli alunni potranno non solo seguire lezioni e compiti, ma anche rimanere in contatto visivo con la propria classe, con innegabili vantaggi dal punto di vista psicologico e didattico. Il corso di sostegno e il supporto alla videocamera saranno erogati mediante CleverPath Portal di Computer Associates.

RICERCATORE, NON PEDOFILO

Un recente, clamoroso fatto di cronaca riguardante la lotta alla pedofilia, che denota quanto, a volte, seppure si tratti di tematica estremamente grave e delicata, si dimentichi un po' il senso comune, si è concluso positivamente. L'autore di un libro sull'argomento, che ha visto aumentare smodatamente il polverone attorno a sé per il suo nome illustre (Pete Townshend, chitarrista degli Who, storico gruppo rock britannico) era stato accusato di aver scaricato immagini di pedofilia dalla Rete, e a nulla erano valse le sue ragioni di "ricerca". Townshend, da sempre impegnato nella lotta alla pedofilia e autore di altri scritti precedenti sull'argomento, aveva effettivamente visitato un sito Web di quel tenore, lasciando persino i dati della propria carta di credito, attraverso i quali la polizia era facilmente riuscita a risalire a lui. E' stato comunque scagionato, con la sola macchia di una ammonizione formale (la pena sarebbe stata di cinque anni di prigione e soprattutto la reputazione irrimediabilmente macchiata), forse anche, diciamolo pure, grazie al suo nome illustre.

FLASH SENZA BROWSER

Con il nuovo tool Macromedia Central, Flash esce dagli angusti limiti del browser e arriva a creare vere e proprie applicazioni ad alto livello di interattività, che possono girare direttamente sul desktop e anche in modalità offline. E non parliamo di giochi, brevi filmati o animazioni varie, ma di tutte quelle applicazioni, come quelle basate sui moduli, che richiedono un inserimento o una visualizzazione di dati dinamici. Con Macromedia Central, tali dati vengono conservati nella cache dopo il loro inserimento nel modulo relativo, e sincronizzati e aggiornati non appena l'applicazione può disporre di una connessione alla Rete.
Questa soluzione è applicabile fra l'altro a previsioni meteo, listini di borsa e news, e si dimostra particolarmente adatta a sistemi mobili, per i quali l'esigenza è la rapida consultazione proprio di questo genere di servizi, senza però disporre di lunghi tempi di connessione.

CENTRINO SU LINUX, FORSE

Intel promette un prossimo, pieno supporto di Linux su Centrino, con l'imminente rilascio dei driver necessari. Ma, al di là dei test della casa madre, non ci sono notizie precise su date di rilascio, e neppure sulla formula che sarà adottata per la distribuzione (commerciale o open source). Intel comunica al proposito che attende un riscontro effettivo dal pubblico, dal quale dipenderà l'effettiva produzione dei driver.

MOZILLA, PUNTO E A CAPO

Il quinto compleanno di Mozilla, caduto il 31 di marzo, coincide con una svolta epocale da parte dei suoi programmatori. Particolare attenzione sarà volta alla semplicità e leggerezza delle applicazioni, che avranno le dimensioni più ridotte possibile. A tale fine, Mozilla abbandonerà la piattaforma di sviluppo Xpfe per appoggiarsi all'architettura Phoenix, su cui si sta sviluppando da tempo una implementazione di Mozilla molto leggera, oltre che il client di posta elettronica Thunderbird, che verrà ufficialmente adottato.
Secondo i programmatori, questa piccola rivoluzione era più che dovuta, visto che oltretutto lo stesso motore di Mozilla, Gecko, aveva bisogno di una massiccia razionalizzazione e di un approfondito bugfix. L'idea ora è quella di puntare su una riduzione ai minimi termini dell'allestimento di base, dando poi ampia disponibilità di plugin.
Il passaggio a Phoenix e Thunderbird avrà luogo fra l'uscita della versione 1.5 (prevista per metà agosto) e della 1.6, mentre l'imminente 1.4 (già uscita in alpha) sarà l'ultima versione stabile basata sul vecchio codice di Mozilla 1.0.

CERCHI GLI ALIENI? OCCHIO AL BACO!

Nessuno è esente da errori. Neppure lo storico progetto SETI@home, in cui, ricordiamo, la potenza di calcolo dei computer connessi in Rete e momentaneamente inattivi viene utilizzata per scandagliare il cosmo alla ricerca di forme di vita, che ha recentemente corretto vulnerabilità di sicurezza sia nel client che nel server. "Banali" buffer overflow i due bug del client, che sono comunque, secondo i responsabili, poco sfruttabili, in quanto si dovrebbe prima convincere l'utente a collegarsi ad altro server, cosa piuttosto inapplicabile in questo caso. Decisamente più serio quello del server, che potrebbe essere sfruttato per condurre attacchi DDOS o, in certi casi, attacchi multipli ai client connessi al server, sfruttando, questa volta con maggiore successo, i bug rilevati nel client. Il server è stato ovviamente patchato e aggiornato, mentre del client è disponibile una nuova versione, la 3.08, per Windows, Linux, Macintosh e tutte le piattaforme supportate, che vede corretti i bug succitati.
Ricordiamo, per la cronaca, che al progetto SETI@home partecipano attivamente 4,4 milioni di utenti, fra cui quasi 8.000 italiani.

NON SI E' PIU' SICURI DA NESSUNA PARTE

Vedere un sarto che va in giro malvestito o un ciabattino scalzo, non stupisce nessuno, lo dice anche un vecchio adagio. Ma scoprire che il Cert Coordination Center, uno dei team di sicurezza su Internet più accreditati nel mondo, patrocinato nientemeno che dal Governo Federale degli Stati Uniti, è stato violato, beh... lascia, se non segretamente compiaciuti, quantomeno parecchio perplessi. Ebbene sì: a metà marzo, sulla mailing list del negli archivi Full Disclosure sono comparsi anzitempo tre post relativi ad altrettante vulnerabilità su cui i vendor e il Cert/Cc stavano lavorando in forma strettamente privata. Brutto affare. La spiegazione dell'accaduto data dal responsabile Sean Hernan, che ha parlato di una disclosure dovuta a una o più persone già in possesso di un accesso sul repository del Cert, non è piaciuta all'autore dell'audace gesto. Hack4Life, così si è firmato l'intruso, ha subito messo le cose in chiaro postando un messaggio inequivocabile: "La conoscenza delle vulnerabilità non deve aiutare gli amministratori di sistema, ma gli hacker e chi le deve utilizzare". Ci mancherebbe che dopo tutta la fatica fatta a violare il sistema, il merito se lo piglia qualcun altro.

DUKE NUKEM 3D OPEN SOURCE

L'occasione del CeBIT è ghiotta per tutti, e Siemens ha voluto a sua volta presentarsi con una ricca gamma di novità.
SL55 è un GPRS tribanda, molto leggero e dotato di display a colori, vivavoce e comandi vocali. Supporta MMS, Java una fotocamera opzionale.
M55 supporta una gestione avanzata delle suonerie e dei temi musicali degli MMS, avvalendosi niente meno che del noto software di sintetizzazione Cubasis. Anche in questo caso troviamo il supporto a Java, il vivavoce e i comandi vocali.
Ma Siemens non vuol dire sono cellulari, ma anche schermi, per esempio. Uno schermo touchscreen tridimensionale che interpreta la distanza fra il display e il dito e visualizza di conseguenza i contenuti, un altro schermo sottile al punto da essere arrotolabile. Poi il mouse per cellulare, che si avvale di una microtelecamera per trasmettere i propri movimenti. E infine una lunga serie di accessori per implementare le funzioni di Gps sui telefoni cellulari.

UNA LEZIONE AI DIALER

Una lezione impartita dall'Australia, che intende porre un freno al diffondersi sempre più massiccio degli infernali softwarini che si barcamenano sulla sottile linea fra il legale e l'illegale. Il funzionamento è ormai noto a tutti: il dialer disconnette il più o meno ignaro installatore (il disclaimer che avverte di quello che sta per accadere è spesso assente o ben nascosto) dalla propria connessione e lo ricollega a un costosissimo numero tipo 166 o simili. E il programma che lancia il dialer è di solito camuffato in pagine allettanti, piene di donnine seminude o suonerie per cellulare.
Telstra, uno dei principali provider di telefonia australiani, ha letteralmente tagliato i ponti alle aziende che si avvalgono dei dialer, avvisando che entro sei mesi sospenderà il servizio. Inoltre tutti gli operatori stanno pensando di tenere sotto controllo i conti telefonici degli utenti, monitorando eventuali sbalzi nella tariffazione, che potrebbero indicare l'utilizzo involontario di un dialer.

BLOG IN VIVA VOCE?

Gekolab Mobile, azienda specializzata in servizi di intrattenimento per piattaforme mobili, ha ideato Audioblog, che consente di aggiornare un blog anche via telefono, e ugualmente permette a chi lo voglia di "sfogliare" un blog via telefono, ascoltando i messaggi vocali lasciati dall'autore. Il servizio può essere utilizzato su qualsiasi sito, appoggiandosi sui server dell'azienda, e costa 1,5 euro per ogni messaggio pubblicato (che non può superare i 30 minuti), più i costi di chiamata; i costi vengono addebitati in bolletta o vengono scalati dal credito del cellulare.

LA MINACCIA DI GANDA

Piccoli worm crescono: questo nuovo volto del massmailing virale dispone nientemeno che di un proprio SMTP engine. L'attachment infetto giunge in forma di screensaver delle dimensioni di 62 Kbyte, allegato a un messaggio in inglese o in svedese, e un comando IFRAME incorporato tenta di eseguire automaticamente l'allegato; una volta in memoria, il worm cerca di terminare gli antivirus residenti.

FALLA NELL'APPLICATION SERVER DI SUN

Sun ONE Application Server è affetto da una grave vulnerabilità di buffer overflow, che potrebbe consentire a un cracker di prendere il controllo del server. Il baco si annida nel Connector Module di Sun ONE (iPlanet) Application Server 6.5 e 6.0. La vera brutta notizia è che la patch sarà rilasciata solo per la versione 6.5: la stessa Sun sostiene che l'utenza della vecchia versione sia troppo limitata per prendere provvedimenti.

Il lato oscuro dell'email

Punti deboli e difese facili per il mezzo di comunicazione che ha rivoluzionato questo mondo e creato un certo scompiglio anche nel regno dei Klingon.

Melissa Klez
Via Code Red 07-20
Backdoor
P.S.: I love you

Ha fatto una pensata nel 1971 e da quel momento non ha smesso di sorridere. Ecco il faccione di Ray Tomlinson, l'inventore dell'email. Potete ritagliarlo e tenerlo accanto al piccì, si dice che porti fortuna...

L'email è nata prima di Internet, quando i computer collegati erano pochi e il network si chiamava ARPANET, e chi l'ha inventata non pensava che nel giro di pochi anni sarebbe stata **usata per la maggior parte delle comunicazioni planetarie, più dei fax e molto più dei sistemi tradizionali**.
Molti dei pregi e moltissimi difetti dell'email derivano dal fatto che, mentre i telefonini, per fare un esempio, sono passati da una tecnologia a un'altra e poi a un'altra ancora nel giro di pochi anni, **il sistema della posta elettronica funziona più o meno nello stesso modo da quando è stato inventato**. A fare la pensata è stato Ray Tomlinson, che nel 1971 ha scritto due programmini, SNDMSG e READMAIL, che funzionavano così così ma che avevano dentro tutto quello che serve per scrivere, spedire e leggere messaggi. Da quel momento il sistema è stato via via potenziato e perfezionato, ma ancora adesso i server di posta sono accessibili da una finestra di terminale e rispondono a comandi tipo HELO, MAIL, QUIT e via dicendo.
Questo significa due cose: la prima è che comunicare via email è possibile da qualsiasi computer che abbia un sistema operativo qualsiasi, un modem qualsiasi e un qualsiasi processore, anche uno preso dalla tastiera di un ascensore. La seconda cosa è che la sicurezza del sistema, per come è fatto, è più o meno quella che ci si può aspettare guidando una 127 sulla tangenziale: poca.

>> Testo e solo testo

Quella di spedire i file allegandoli ai messaggi di posta elettronica è un'idea che è venuta dopo, quando il sistema era già bello che formato ed **era fatto su misura per spedire - testo - e - solo - testo**. Pur di far contenti gli utilizzatori del sistema, sono stati studiati algoritmi di codifica e decodifica che, indipendentemente dalle sigle che hanno, traducono i file allegati in modo che riescano a passare attraverso computer che si aspettano di ricevere e ritrasmettere testo. Le debolezze del sistema sono semplicemente nella sua natura, e per un server mail può passare il peg-

Benché la notizia abbia dell'incredibile, pare che la tennista Anna Kourikova non stia affatto spedendo in giro per Internet foto in pose particolari per farsi amica dei navigatori della Rete…

giore dei virus come un canto della Divina Commedia, lui lo codifica, lo decodifica e lo recapita.
Approfittarsi di questo fatto è come rubare le caramelle ai bambini, ma proteggersi è altrettanto facile, basta sapere dove stanno i veri pericoli.

>> Istruzioni pericolose

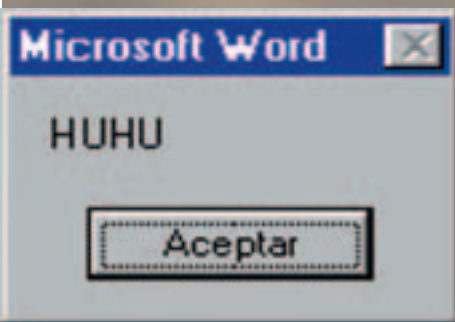
Più un programma è diffuso, più è facile che un virus che lo attacca si diffonda in Rete. Se poi il programma è pure "scemo" e i danni se li fa quasi da solo siamo proprio a posto. Il bello è che un programma del genere esiste davvero ed è pure uno dei più usati, visto che lo troviamo dentro a un sistema operativo. **Aggirare le difese di Outlook è facilissimo: basta mettere uno script maligno dentro a un messaggio formattato in HTML** e Outlook, con le regolazioni di base, manco lo deve aprire: si "infetta" **direttamente mentre mostra l'anteprima**. I virus che funzionano in questo modo sono allegati ai messaggi con nomi invitanti (Anna Kournikova) oppure sono infilati dentro al codice HTML dei messaggi stessi sotto forma di script, per esempio.
Se il pericolo si annida in un allegato, è necessario farci un doppio clic per infettare la macchina. Per farci doppio clic bisogna **non riconoscere il file come pericoloso**, e così nomi invitanti, estensioni camuffate e cose del genere spesso traggono in inganno.
Una volta eseguito, il virus, che spesso è un Worm, che si propaga a dismisura attraverso le macchine che infetta danneggiando file qua e là, un Trojan, che apre le porte del computer al suo gentile padrone, che non sempre è il mittente, oppure un Macro virus, che combina danni più o meno gravi sfruttando i codici usati in Word, Excel e simili, **può essere eliminato solo con un antivirus o con la cancellazione di tutti i file ai quali si è attaccato**.

>> Come difendersi

Difendersi dai pericoli della posta elettronica è appena un pochino meno facile che farsi fregare, ma basta poco.

1. non aprire file con estensioni 386, BIN, CMD, COM, DEV, DLL, DOC, DOT, EXE, INF MD?, MPP, MPT, OBT, OLE, XL?, VXD, OVL, PP?, POT, PIF SCR, SHS, SYS, VBS, XPT senza averli controllati con un antivirus aggiornato.
2. disattivare qualsiasi funzione di visualizzazione automatica, compresa l'anteprima messaggi, del programma di posta.
3. installare e tenere aggiornato un antivirus decente, senza credersi per questo autorizzati a buttarsi alla cieca su qualsiasi cosa si possa scaricare dalla Rete.
4. installare e tenere aggiornato un firewall decente. Qui abbiamo chiesto ai nostri di Hackers Magazine e abbiamo qualche indicazione decisiva: date un'occhiata nei loro CD.
5. evitare di credere a cose che se ve le dicessero a voce ridereste ma dato che sono scritte sembrano più vere.
6. utilizzare un server di posta che faccia un minimo di controllo antivirus, per esempio quello di Yahoo, per trasferire allegati.
7. scegliere un programma per la posta che non sia il più diffuso al mondo, visto che i virus si propagano attraverso organismi, e macchine, omogenei.
8. scegliere sistema operativo e programmi per scrivere e far di conto con lo stesso criterio usato al punto 7.
9. leggersi qualche rivista che non abbia paura a dire le cose, ma questo è opzionale.

>> email sicura e asini che volano

La posta elettronica è fatta per spedire testo da un computer a un altro, **nessuno dei suoi inventori si è mai preoccupato del rischio che qualcuno mentisse nel mandare un messaggio email**, semplicemente perché, nella logica del sistema, questa cosa non ha alcun senso. Chi mai può essere interessato a mandare un messaggio senza poter ricevere una risposta? E chi mai potrebbe aver voglia di fingersi un altro per scrivere a qualcuno? A un popolo di brillanti ma terribilmente onesti ingegneri queste domande suonavano come barzellette, e così **i server di posta non stanno lì a guardare se siete davvero chi dite di essere o altre cose**: loro sono lì per mandare e ricevere posta e quello fanno.
Sapere come è fatto un messaggio di posta elettronica, come viene trasmesso e come viene ricevuto, permette sia di sfruttare meglio alcune funzioni dei programmi che usiamo, sia di smascherare facilmente i messaggi falsi. Già, perché come succede per le lettere scritte, le telefonate e mille altre cose, **c'è chi si diverte pure a falsificare le email o a moltiplicarne il flusso in modo da creare confusione nella nostra casella e nei vari server**.
Ogni email è costituita, oltre al corpo del messaggio, da un indirizzo di desti-

Una bizzarra variante del macrovirus Melissa ha appena colpito una macchina e la saluta simpaticamente. Immagine scattata in Spagna.

nazione, un mittente, un subject e una serie di informazioni sul suo percorso dalla partenza all'arrivo. Questi dati di solito sono nascosti, i programmi di posta mostrano appena il mittente e il destinatario, ma se li guardiamo da vicino possono raccontarci un sacco di cose interessanti.Da: `Piero@posta.it`
Indica il mittente. Si basa sulle informazioni contenute nel programma di posta e non ha molta importanza dal punto di vista tecnico, potrebbe contenere qualsiasi cosa e il messaggio partirebbe lo stesso.

`Data: Mer 9 Apr 2003 12:27:58 Europe/Rome`

È la data in cui il messaggio è stato spedito. Anche questa viene inserita dal programma che invia la posta, e quindi si basa sulle regolazioni del computer di chi ci scrive. Questo significa che, a volte, arrivano messaggi con date improponibili, tipo 1910 o 2230. Non si tratta di fenomeni paranormali, ma solo di personaggi un po' distratti che avranno grossi problemi se un giorno decidessero di fare dei backup. L'ora e il fuso orario possono essere regolati in maniera giusta o sbagliata, il messaggio parte e arriva ugualmente.

`A: redazione@hackerjournal.it`

Questo è il campo del destinatario, e quello che c'è scritto qui è decisivo per l'arrivo del messaggio. Il fatto che ci sia un indirizzo in questo campo, però, significa solo una cosa: che se quell'indirizzo è valido il suo proprietario riceverà il messaggio.

`CC: grAnd@hackerjournal.it`

Qui troviamo gli indirizzi di chi riceve il messaggio in copia. Mettere un indirizzo in questo campo o metterlo nel campo A è la stessa cosa.

`BCC: piero@serverposta.com`

Questo campo è visibile solo a chi spedisce il messaggio. È possibile che tutti gli indirizzi dei destinatari siano qui e che nel campo A: ci sia lo stesso indirizzo del mittente, la cosa funziona in modo egregio e nessuno saprà se altri hanno ricevuto l'email.

`Oggetto: gli header`

Qui ci va il titolo del messaggio, in inglese questo campo si chiama Subject. Lasciarlo in bianco è una pessima abitudine.

`Reply to:piero@serverposta.it`

Questo indirizzo è quello a cui verranno inviate eventuali risposte al messaggio. Anche questo campo può contenere informazioni valide o non valide e il messaggio arriva lo stesso. Ma se l'indirizzo specificato qui è sbagliato le risposte non arriveranno mai. È interessante notare che, se nel campo del mittente inseriamo un nome di fantasia e qui ci mettiamo il nostro vero indirizzo, le risposte arrivano lo stesso ma quel che si vede all'arrivo del messaggio è il nome di fantasia.

```
Received: from smtp.hacker-journal.it(193.74.144.44) by imsa.hackerjournal.it (7.0.012) for redazione@hackerjournal.it; Wed, 9 Apr 2003 12:25:49 +0200
Received: from n11.grp.scd.yahoo.com (66.218.66.66) by smtp.serverposta.it (7.0.012) for redazione@hackerjournal.it; Wed, 9 Apr 2003 12:25:49 +0200
```

Qui ci sono informazioni più interessanti. Queste righe indicano il percorso che ha fatto il messaggio dal punto più vicino a noi a quello più vicino al mittente. Possono esserci dozzine di indicazioni come questa, ciascuna indica una tappa che il messaggio ha fatto presso un server che lo ha inoltrato e l'ora a cui questo è avvenuto.

CIFRATURA GRATIS PER TUTTI

La cifratura di Zimmermann ha aperto una nuova frontiera, quella della firma elettronica e della sicurezza dei documenti digitali. A rendere disponibile a tutti questo servizio ci ha pensato, per quel che riguarda la posta elettronica, HushMail www.hushmail.com. Usare Hushmail non è un piacere, è un dovere morale. Intanto perché qualsiasi mail e qualsiasi file che passi di là viene crittografato con una chiave spaventosamente sicura e protetto da una passphrase, che non è una password, sono tante password una in fila dietro l'altra, poi perché un messaggio, anche con allegati, che viaggia da un account Hushmail a un altro account Hushmail è tra le cose più sicure che si possano fare con un mouse e una tastiera, e poi perché non costa nulla. L'account base di Hushmail, con indirizzo e spazio per i file, è gratis e gratis rimarrà.
Se qualcuno vi propone programmi o servizi a pagamento per cifrare i vostri messaggi, provate per bene la versione freeware di PGP e l'account base di Hushmail, chi vi scrive sono anni che va avanti con quelli, si trova benissimo e non ha mai sborsato una lira, finchè c'erano le lire.

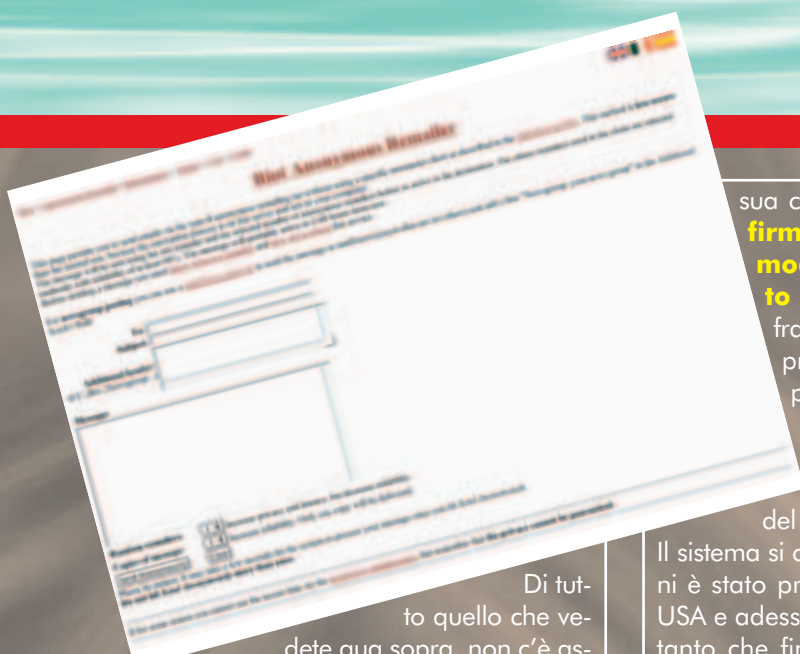
`X-Sender: Piero@posta.it`

Questo è l'account usato dal mittente per spedire il messaggio.

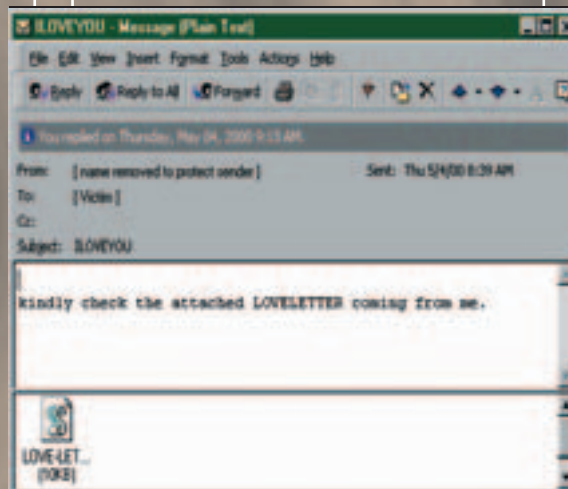
`X-Mailer: Lotus Notes Release 5.0.9 November 16, 2001`

Questo è il programma di posta usato per spedire il messaggio.

`Message-Id: <OPB3ANAD9A.1D40CFCD-ONC1256D03.0038FD43@posta.it>`

Questo è il codice univoco che identifica il messaggio.

Di tutto quello che vede qua sopra, non c'è assolutamente nulla che non si possa falsificare, mascherare o truccare in qualche modo; sappiatelo.
Per mascherare la nostra identità **possiamo spedire un messaggio email tramite server specifici, detti remailer anonimi**. Ce ne sono diversi in Rete, per provarne un paio andiamo a http://riot.eu.org/anon e a http://freedom.gmsociety.org.
Le mail che arrivano tramite questi servizi non sono tracciabili, cioè non si può risalire al vero mittente se non con indagini degne di un ufficio dei servizi segreti (che peraltro riescono benissimo a venire a capo anche di questi segreti incrociando dati qua e là).

>> La soluzione è altrove

Tanto per cambiare, invece di fare mille tentativi per costringere un sistema a fare qualcosa che non era nel piano di chi lo ha inventato, per risolvere un problema c'è voluto qualcuno con un'idea del tutto nuova. Quel qualcuno si chiama Phil R Zimmermann e **ha inventato qualcosa di geniale: la crittografia a chiave pubblica**.
Il sistema funziona in modo semplice: ciascuno ha una chiave privata segreta e una chiave pubblica che distribuisce a tutti. **Per essere sicuri che un nostro messaggio venga letto solo da una persona**, noi possiamo cifrarlo con la sua chiave pubblica (che abbiamo) e lui può decifrarlo con la sua chiave privata, mentre **per firmare un messaggio in modo assolutamente certo** basta che usiamo una cifratura con la nostra chiave privata: solo la nostra chiave pubblica farà scattare il meccanismo e, rendendo leggibile la firma, garantirà provenienza e integrità del messaggio.
Il sistema si chiama PGP, per diversi anni è stato protetto da segreto militare USA e adesso è di libera distribuzione, tanto che finalmente Zimmermann si è potuto comprare una casa e una macchina decenti dopo anni che non riusciva a cavare un dollaro dalla sua invenzione.
Per usare PGP basta poco, perché da quando è diventato "legale" è anche diventato "commerciale" e **se prima si faceva tutto da riga di comando adesso basta un clic e firmi, cifri, decifri, verifichi un messaggio in un baleno**. Per prelevare la versione freeware di PGP basta andare al sito www.pgp.com. Il programma può essere usato anche per cifrare file o cartelle in qualsiasi sistema operativo, per firmare documenti scritti con Word o per "bloccarli" impedendo eventuali modifiche, per proteggere dati e per fare un sacco di cose altrettanto divertenti.
Se invece la linea di comando non vi spaventa, e preferite un software libero in tutto e per tutto, provate GPG, Gnu Privacy Guard: lo trovate all'indirizzo www.gnupg.org.

GRANDI FAMIGLIE DI VIRUS

Macro virus: si attaccano ai documenti Office e viaggiano con loro, si diffondono molto velocemente e possono essere difficili da fermare anche dopo che sono stati scoperti. In compenso, con un po' di prudenza e disattivando l'esecuzione automatica delle macro e l'anteprima nei programmi di posta è difficilissimo venirne colpiti. I campioni sono: W97M/Melissa e le sue varianti, W97/Brenda, WM/Wazzu, O97M/Y2K.

Worms: non si attaccano ad altri file ma tendono a replicarsi autonomamente attraverso i contatti che trovano nella rubrica di posta, possono fare danni molto gravi e sono piuttosto veloci, tanto che molti virus tra i più diffusi sono proprio worms: W32/SQLSlammer, W32/Oror e varianti..

Virus di boot: questi non attaccano i file ma direttamente i dischi. Un tempo erano molto più pericolosi, perché lo scambio di floppy e di dischi era l'unico modo per trasferire velocemente file. Per la storia, citiamo il famoso e illustre AnitCMOS, che riscriveva a modo suo il settore di avvio dei dischi che trovava sulla sua strada.

Trojan: aprono una porta di comunicazione e di controllo nel computer che raggiungono. Alcuni Trojan, come SubSeven, possono essere usati come alternativa economica ai programmi di controllo remoto, anche se le caratteristiche si sicurezza dell'accesso che offrono non sono eccellenti. Oltre a SubSeven citiamo i dannosi BackOrifice_2000 e Vampire.

COME TROVARE INFORMAZIONI SU INTERNET

UUFMDR:

Non capite perché su Irc vi prendono in giro quando chiedete da dove si può scaricare WinMX? Magari è meglio se, prima di chiedere, cercate da soli le risposte più ovvie.

Molti di voi penseranno che un articolo su come si fa una ricerca su Internet è di livello troppo basso per una rivista come questa. Il fatto è che **ogni tanto arrivano in redazione richieste imbarazzanti**, non tanto per l'argomento (ormai non ci scandalizziamo più di niente), ma piuttosto perché si tratta di domande la cui risposta può essere trovata in meno di un secondo (pochi centesimi di secondo, per essere precisi). Credete che esageriamo? Volete un esempio?
Domanda: "dove posso trovare un tutorial in italiano sul programma CDex per estrarre Mp3?"
Risposta: segui il primo link che compare in Google, inserendo le parole: cdex tutorial italiano. Google impiega 13 centesimi di secondo per fornirla. **Non è più pratico che scrivere a noi, e aspettare la risposta via email?**
Quindi, vediamo di ripassare un po' i fondamentali della ricerca.

>> Le basi

Inserendo una o più parole nella finestra di ricerca, un motore individua nel suo archivio tutte le pagine Web che contengano quella parola (o quelle parole). Inserendo più di una parola, quasi tutti i motori restituiranno pagine che le contengono tutte, ma qualcuno mostra invece le pagine che contengono almeno una tra le parole inserite, allargando inutilmente la ricerca. In questo caso, bisognerà **specificare esplicitamente il tipo di associazione tra le parole, usando l'operatore AND** se vogliamo ottenere pagine che le contengano tutte (**pippo AND topolino AND pluto**), oppure OR se vogliamo pagine che contengano almeno una tra le parole utilizzate nella ricerca (**pippo OR topolino OR pluto**).
A volte, si possono realizzare ricerche molto complesse aggiungendo delle parentesi per racchiudere gli operatori logici. Per esempio, con un'espressione di questo tipo:

```
(pippo OR pluto) AND topolino
```

si trovano le pagine che contengono le parole pippo e topolino oppure pluto e topolino.

>> "Sotto" al Web

Nonostante i principianti tendano spesso a confondere il Web con Internet, i servizi offerti e le informazioni disponibili vanno ben più in là del solo www. Per esempio, ci sono **i newsgroup**: anni e anni di messaggi scambiati sugli argomenti più vari sono immagazzinati e accessibili, ancora una volta, grazie a Google. I newsgroup sono spesso un'ottima fonte per **informazioni, diciamo così, non ufficiali e "underground"**. Molto spesso, le pagine Web con informazioni e link legati all'hacking, **vengono rimosse dai server che le ospitano** (specialmente se gratuiti). Sui newsgroup, invece, queste informazioni passano tranquillamente e, una volta che entrano nell'archivio di Google, ci restano per sempre.
Alcuni newsgroup poi, **quelli delle categorie "binaries", trasportano (spezzettati in svariati messaggi) anche file di vario tipo**: mp3, video, software... Ovviamente, per quanto riguarda gli eseguibili, non ci si può mai fidare: **potrebbero infatti contenere virus o backdoor**, così come qualsiasi programma pirata trovato in Rete. Per cercare nei newsgroup con Google, la pagina di riferimento è
http://groups.google.com

Volete un motore di ricerca con interfaccia hackerosa? Seguite il link "Strumenti per le lingue" di Google e selezionate la lingua Hacker!

>> Trovare file

Altra funzionalità spesso dimenticata è l'ftp, un tempo l'unico protocollo per il download di file. Pochi sanno che esiste un network di server ftp che, analoga-

Volete saperne di più sui motori di ricerca? Ecco due siti pieni zeppi di info, uno italiano e uno americano. Si tratta di Motoridiricerca.it e di searchenginewatch.com.

USATE UN FOTTUTO MOTORE DI RICERCA!

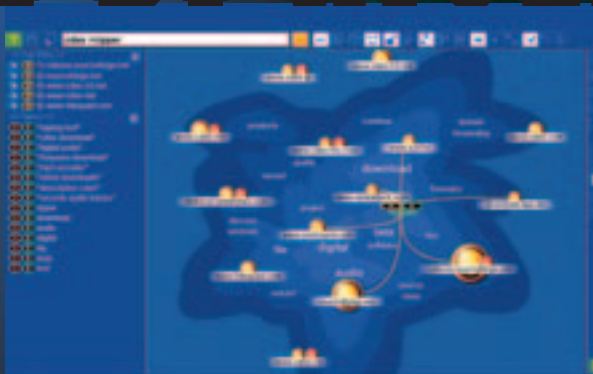
mente a quanto accade con i sistemi peer to peer, rendono disponibili programmi, Mp3 e film da scaricare. Si tratta quasi sempre di **normali computer, con collegamenti dialup, dsl o cable modem**; spesso quindi gli indirizzi cambiano continuamente, e rimangono validi per pochi giorni se non ore. **Dove si trovano questi server?** Beh, nei canali "giusti" di Irc, sui newsgroup, oppure - in modo ancor più semplice - usando un motore di ricerca per server ftp, come per esempio oth.net.

Oth.net funziona più o meno così: chi ospita un server ftp, comunica il proprio indirizzo al sito. Questo analizza le directory, e ne inserisce il contenuto in un database, accessibile attraverso un normale modulo di ricerca dalla home page. **Ogni server può avere una sua politica di accesso**, per cui è possibile che in cambio di un file da scaricare, il proprietario vi richieda di fare l'upload di altro materiale.

Per sapere invece come sfruttare Irc per ricercare file e informazioni su Internet, **fate un salto a pagina 30.**

>> Non solo Google

Sebbene sia sicuramente il motore giusto dove fare un primo tentativo, Google non è l'unico motore di ricerca. In certi casi può essere utile rispolverare qualche vecchia gloria del passato. Per esempio, **con AltaVista si può usare l'operatore NEAR tra due parole**, in modo da restituire pagine in cui le due parole chiave inserite compaiono vicine (pluto NEAR topolino). Questo è molto utile se una delle due parole ha un significato molto generico, e quindi può essere usata in pagine dai contenuti più vari.

Un altro trucco, che vale anche con Google, è quello di **utilizzare le pagine di ricerca avanzata (Advanced search)**, che permettono per esempio di restringere il campo a un certo dominio, cercare documenti in una lingua specifica, o in un posto specifico della pagina (titolo, url, corpo della pagina). Se poi con le ricerche avanzate ci prendete la mano, **non dimenticate di fare una visita a HotBot (www.hotbot.com), che ha funzioni davvero uniche in questo senso**.

Kartoo (www.kartoo.com) è un motore che produce una mappa visuale delle pagine che contengono le parole cercate. L'efficacia è tutta da dimostrare, ma è figoso da morire :)

Volete provare qualcosa di completamente diverso? Fate un giro su Kartoo (www.kartoo.com). Si tratta di un motore che mostra i risultati in modo grafico (grazie a Flash), **creando una mappa che sintetizza la presenza della parola sui vari siti**, e mostra anche parole che accompagnano la parola cercata. Facendo clic sulle parole aggiuntive, si può restringere la ricerca alle pagine desiderate. Più semplice da capire usandolo che da spiegare a parole: provatelo.

>> Approfondire la ricerca

Un errore commesso da molte persone è quello di cercare su un motore generico una risposta troppo specifica o specialistica. Cercare le giuste impostazioni per configurare un modem Usb sotto una particolare distribuzione Linux può essere un lavoro troppo oneroso da svolgere armati di solo Google. In questi casi, conviene forse **usare il motore generico per cercare dei siti che si occupano specificatamente dell'argomento in questione**. Dopodiché, si potrà cercare di utilizzare la funzionalità di ricerca del sito trovato, per vedere se al suo interno contiene le informazioni che cerchiamo. Questo vale soprattutto per i forum, e tutti i siti con aggiornamenti continui: i motori di ricerca infatti possono soltanto fare "fotografie" del sito a certi intervalli di tempo, e **le informazioni più recenti quindi, spesso non sono incluse negli indici**. Molti forum inoltre, configurano il file robots.txt per evitare l'indicizzazione dei contenuti (spesso per evitare consumo di banda e di risorse del server). Anche in questo caso, bisognerà prima trovare il sito, e poi cercare le informazioni al suo interno. Nella prima ricerca, con un motore generico, si possono quindi usare una o due parole chiave, più parole come **forum, community, board** eccetera.

Le opzioni di ricerca avanzata di HotBot sono tra le più sofisticate in circolazione: meritano una visita.

Retrocomputing: alla riscoperta dei computer del passato

A VOLTE RITORNANO

Negli ultimi tempi una parola è sulla bocca di molti, emersa dall'ambito ristretto di smanettoni, tecnofili ed appassionati nostalgici: retrocomputing.

Questo termine riunisce un mondo sfaccettato e vario: c'è chi ricostruisce cabinet da sala giochi, chi recupera vecchi Mac installandovi sopra Linux (www.68k.maximumdebian.org/cgi-bin/index.cgi), chi invece ha il feticcio dell'hardware "nero" e magari colleziona le macchine della scomparsa NeXT (www.channelu.com/NeXT/Black/index.html), chi ancora sogna macchine epocali come l'ALTAIR, l'APPLE I o il LISA, chi perpetua le gesta di sistemi come l'Atari o l'MSX, tuttora vivo ed agguerrito, o chi invece è interessato ai sistemi operativi e alla loro evoluzione (www.mytech.it/mytech/computer/art006010042112.jsp) o al ricchissimo parco software e alla sua conservazione e spinge per promuovere il concetto di "abandonware" (www.mytech.it/mytech/archivio/art006010022137.jsp).

Per quanto possano essere diverse le motivazioni che spingono a ricercare, venire in possesso, riparare, rimettere in funzione, collezionare, quasi tutti i retrocomputeristi concordano sul fatto che dedicarsi a macchine etichettate dagli altri "obsolete" e "superate" è molte volte più interessante che usare i computer attuali. In palio c'è non solo la **riscoperta di un mondo passato, pionieristico e multiforme**, tutto all'insegna della diversità e dell'inventiva ma anche la consapevolezza di star aiutando a **conservare la storia**, una storia che molti ignorano e che sarebbe il momento di conoscere ed apprezzare.

I prezzi? Certo, **c'è chi a fini collezionistici è disposto a sborsare anche parecchi soldi** per un particolare "pezzo raro" o a lanciarsi in aste online, ma perlopiù le somme sono molto ragionevoli, quando non addirittura simboliche, e i luoghi in cui il retrocomputerista "recupera dall'oblio" hardware e software sono cantine, soffitte e solai di amici e parenti, fiere e anche qualche discarica.

>> Manifestazioni

A volte il retrocomputing esce allo scoperto in occasioni per così dire "pubbliche" per mostrare, grazie all'opera degli appassionati, **la straordinaria ricchezza del patrimonio informatico che ci ha preceduto**, anche a vantaggio di chi è informaticamente "giovane".

E' il caso delle prossima "Varese Retrocomputing" (**http://retrocomputing.hal.varese.it), che si terrà domenica 27 aprile prossimo, presso il MUel, il Museo Elettronico di Varese.** Questa prima edizione si articolerà su un intero pomeriggio con interventi di esperti e collezionisti di retrocomputing, che presenteranno, in funzione, numerosi computer che hanno fatto la storia dell'informatica: annunciati anche **diversi pezzi rari come cloni dello Spectrum** (tra cui uno di produzione rumena).

Quello di Varese non è l'unico appuntamento che coinvolge retrocomputeristi: ci sono altre occasioni d'incontro come a Vicenza o gli incontri di Marzaglia due volte all'anno, o le varie fiere del radioamatore e dell'elettronica in giro per l'Italia in cui andare a caccia di pezzi interessanti. Per qualche data rimandiamo al sito di Daniele Gratteri nei link.

Nicola D'Agostino
dagostino@nezmar.com

SITI RETRO'

Computer History Museum
www.computerhistory.org
Ancient Computer Community
www.ancientcomputer.com
Computer Museum .it
www.computermuseum.it
Gli amici di HAL
www.hal.varese.it/computermuseum/homepage
Retro BBK
http://retro.bbk.com
The GUI Gallery
http://toastytech.com/guis/index.html
The Unofficial CP/M site
www.cpm.z80.de/
MSXItalia
http://space.tin.it/computer/enribarb
Retronomicon - Il Libro dei Nomi dei Computer
www.rlyeh.it/Retronomicon/
it.comp.retrocomputing
http://groups.google.it/groups?hl=it&lr=&ie=UTF-8&group=it.comp.retrocomputing
Daniele Gratteri
http://spazioinwind.libero.it/danielegratteri/eventi.html

LINUX FAQ

"Boot, root e swap" non sono suoni da fumetto, ma concetti ed elementi coi quali occorre familiarizzare un po' per riuscire a installare e usare Linux.

Volendo provare Linux, ho scaricato l'ultima versione della Mandrake. Tuttavia non funziona nulla perché inserisco il CD e riavvio la macchina ma il PC carica normalmente Windows. Mi hanno detto che forse il CD che ho masterizzato non è di boot… Che significa? Se provo ad inserirlo sotto Windows non succede nulla… È forse perché ho disabilitato l'autorun?

Attenzione a non confondere Boot e Autorun! Sotto Windows ("Notifica inserimento automatico" vi dice nulla?) è possibile creare dei CD in grado, una volta inseriti, di avviare un determinato programma; nulla a che vedere però con i CD di boot, ovvero in grado di avviare il sistema da CD. In primo luogo occorre sincerarsi di aver inserito nel lettore il primo CD della distribuzione e non uno qualsiasi, poiché solitamente solo quest'ultimo è di boot. Inoltre, molto probabilmente, il PC è stato impostato per avviarsi da Hard Disk e non da CD. È necessario quindi entrare nel BIOS del proprio PC e impostarlo in maniera tale che si avvii dall'unità CD-Rom; esistono però molti BIOS differenti e non esiste un menù standard dove poter fare questo, ma cercate qualcosa del tipo "First Boot Device" o "Boot Sequence" ed impostate il CD-Rom come primo dispositivo.

>> Ritorno al floppy

Il BIOS della mia scheda madre è piuttosto vecchiotto e non consente di avviare il sistema da CD; è possibile creare un floppy di boot (come succede per Windows)?

Se il vostro computer non è grado di fare il boot da CD-Rom, potete ovviare a questo inconveniente creando un

floppy di Linux avviabile che provvederà automaticamente a caricare i driver del CD, permettendovi quindi di proseguire nell'installazione. Procuratevi pertanto un paio di floppy (meglio se vuoti, sappiate comunque che tutto il loro contenuto verrà perso!) e inserite il primo CD della vostra distribuzione. Iniziate a sfogliare il suo contenuto alla ricerca di una cartella \dosutils; al suo interno troverete sicuramente un programma chiamato rawrite o rawritewin (il primo funziona sotto DOS mentre il secondo, disponibile all'indirizzo http://uranus.it.swin.edu.au/~jn/linux è progettato per Windows). Questi programmi servono per scrivere su un floppy un'immagine dei dati; quello che ci serve è quindi un immagine avviabile da poter scrivere… Solitamente le distribuzioni dispongono di una cartella \images, \disks o \bootdisk contenente appunto diverse immagini; fate riferimento al ReadMe presente nella stessa cartella, ai manuali acclusi o alla documentazione on-line per identificare quale fa al caso nostro (solitamente boot.img o cdrom.img…). Infine avviate rawrite, indicate il percorso completo dell'immagine che volete scrivere e la lettera dell'unità floppy di destinazione; a questo punto dovrete semplicemente riavviare lasciando CD-Rom e floppy inseriti ed attendere che il dischetto avvii il sistema.

>> Quante partizioni figliolo?

Salve! Non sono ancora riuscito a capire quante partizioni bisogna fare… Qualcuno mi dice che ne basta una sola, qualcuno addirittura 4! Ed è vero che c'è un ordine particolare? Fondamentalmente Linux è in grado di funzionare perfettamente utilizzando la sola partizione di root e appoggiandosi a una partizione di Swap per la memoria virtuale (consigliato!). Per un utilizzo "domestico" questo schema, data anche la sua estrema semplicità, è decisamente consigliabile; in taluni casi tuttavia è preferibile adottare un partizionamento più complesso. Partizioni contenenti per esempio i dati personali dei vari utenti o tutta la posta e le code di stampa accumulatesi possono essere mantenuti inalterati su una partizione

dedicata anche in caso di reinstallazione del sistema, e in seguito montati nel filesystem, così da rendere molto più semplice il salvataggio dei dati; inoltre, partizioni diverse possono utilizzare filesystem diversi. Per ottenere migliori prestazioni, si consiglia di disporre le partizioni in un determinato ordine, partendo da quelle con una maggior frequenza di accesso; un esempio di partizionamento (ideale ad esempio per un server) potrebbe essere, nell'ordine, Swap, /usr, /var, / e /home.

>> Scambio di memoria

A che serve la Swap? Quanto deve essere grossa la partizione di Swap? E se volessi aumentarne la dimensione senza ripartizionare l'intero hard disk?

Linux supporta la memoria virtuale, permettendo cioè di utilizzare spazio su disco come se fosse un'espansione di memoria RAM e aumentando di conseguenza la dimensione massima di memoria utilizzabile. Sebbene i programmi vedano un'unica memoria avente come dimensione totale la somma degli spazi disponibili, i tempi di accesso per la lettura e la scrittura dei dati contenuti su hard disk sono di gran lunga superiori di quelli per l'accesso alle memoria RAM; per questo motivo il kernel tende a liberare spazio in memoria salvando su disco i blocchi che in quel momento non sta utilizzando, così da poter

Talor lasciando le sudate carte…

La quantità di documentazione (guide, manuali, pagine help, Faq, How-To, tutorial etc) disponibile per Linux è ingente e, come abbiamo visto nella puntata precedente, esistono progetti nati appositamente con lo scopo di ordinare tutti questi testi. Tutta questa documentazione può venir però resa disponibile in diversi formati, alcuni molto diffusi e altri più esotici…

man Il formato tradizionale, estremamente semplice ma altrettanto funzionale, di documentazione sui comandi e sui programmi

in ambiente *nix; le pagine di manuale forniscono infatti informazioni sul funzionamento, sulle loro opzioni o sulla configurazione dei programmi.

Texinfo Il formato ipertestuale adottato ufficialmente dal progetto GNU per la documentazione del sistema e pensato per sostituire man.

HTML Il linguaggio standard per la documentazione consultabile tramite un Web Browser testuale o grafico. Solitamente, insieme alla versione ipertestuale, viene fornito l'intero documento in un'unica pagina per un'eventuale rapida consultazione anche off-line.

RTF, Puro Testo Semplici e senza troppi fronzoli ma poco pesanti e facilmente leggibili su qualunque piattaforma, questi formati non vi tradiranno mai; inoltre, a differenza dei DOC, non possono trasformarsi in facili portatori di Macro Virus… :)

PS, PDF, DVI, TeX Per aprire i file di stampa PostScript potete utilizzare Ghostscript (http://www.cs.wisc.edu/~ghost/), utile anche per aprire i PDF (per questi file esistono però anche Adobe Acrobat per Linux o xpdf - http://www.foolabs.com/xpdf/); TeX è invece un software per la composizione tipografica e i file che produce sono in formato DVI (leggibili con il programma xdvi).

Infine considerate che molto spesso documenti molto voluminosi o composti da più file vengono raccolti e diffusi come un unico file compresso, avente estensione .tar.gz o gzip. Non c'è che dire: avete solo l'imbarazzo della scelta! Buona lettura…

Sfogliando il pinguino...

Tra i tantissimi libri riguardanti il funzionamento e l'utilizzo di Linux che invadono oggi gli scaffali delle librerie, ve ne vogliamo presentare un paio decisamente particolari...

Il primo, "**Linux - Guida per l'amministratore di sistema"** (edito da Hops Libri), è stato scritto da Lars Wirzenius, tra i fondatori del Linux Documentation Project, e tradotto da Eugenia Franzoni, personalità di spicco del Pluto Linux User Group. Gli argomenti sono trattati in maniera sintetica ma estremamente chiara: si passa da una panoramica sui componenti del SO (kernel, demoni...) a un'analisi dettagliata del filesystem standard di Linux, per arrivare poi a capitoli dedicati al funzionamento e alla gestione dei diversi dispositivi di memorizzazione o alla memoria virtuale. Ogni amministratore (o aspirante tale) di sistema non potrà inoltre non divorare i capitoli dedicati al login e alla gestione degli account, all'avvio e all'arresto del sistema o ai backup (tra l'altro, i lettori di Hacker Journal hanno diritto a uno sconto del 15% sull'acquisto online di tutti i libri pubblicati da Hops Libri. Visitate il nostro sito per scoprire come ottenere lo sconto!)

Linux Problem Solver, edito da Mondadori Informatica, è invece un volume dedicato a coloro che vogliono sfruttare al massimo le potenzialità di questo sistema operativo risolvendo in maniera semplice ed elegante i piccoli o grandi problemi che spesso si presentano. Oltre cento problemi connessi all'amministrazione, la configurazione, l'aggiornamento o la manutenzione dell'intero sistema offrono lo spunto per approfondire una determinata tematica. Inoltre l'autore è Brian Ward, autore del "Linux Kernel HOW-TO", e allegato al volume potrete trovare un CD contenente un sacco di software interessante, utility per il ripristino in caso di emergenza e tutti i Linux HOW-TO.

utilizzare la memoria per altri scopi e poter comunque recuperare all'occorrenza da disco i dati originali. La dimensione ottimale di questo apposito spazio su disco, chiamato spazio di swap (che in inglese significa scambio), dipende da molti fattori: la quantità di memoria Ram presente, l'utilizzo che verrà fatto del sistema, la velocità di rotazione del disco e la versione del kernel. In linea di massima è consigliabile creare una partizione di swap avente dimensione doppia di quella Ram, anche se ad un certo punto, all'aumentare delle dimensioni della swap, non corrisponde più un sostanziale incremento delle prestazioni; per una normale postazione di lavoro 264 MB saranno sufficienti e sarebbe comunque poco conveniente spingersi oltre i 512 MB.

Talvolta può accadere di aver bisogno per un breve periodo di tempo di una quantità di memoria elevata; fortunatamente è possibile creare un file di scambio momentaneo da poter utilizzare senza dover ripartizionare il disco, anche se l'accesso a un file di scambio richiede tempi superiori rispetto all'accesso ad una partizione dedicata. Supponiamo quindi di voler creare nella directory /dev un file di swap di 10 MB chiamato extraswap e avente blocchi di 1024 byte: dovremo prima creare con il comando 'dd' un file vuoto, formattarlo con 'mkswap' e infine attivarlo o disattivarlo all'occorrenza... Ecco in dettaglio come fare:

```
 # dd if=/dev/zero
of=/dev/extraswap bs=1024
count=10000
 10000+0 record in
 10000+0 record out
 # kswap /dev/extraswap
10000
 Setting up swapspace ver-
sion 1, size=9996Kb
 # sync
 # swapon -v /dev/extraswap
 swapon on /dev/extraswap
 ....
 # swapoff -v /dev/extra-
swap
 swapoff on /dev/extraswap
```

>> L'importanza di chiamarsi root

Aiuto, non riesco ad installare il pacchetto XYZ!! Perché non riesco a compilare il tale o il tal altro modulo? Volevo modificare un'impostazione di sistema: mi hanno detto che devo andare a modificare un determinato file in /etc, ma il sistema mi dice che non sono autorizzato a farlo... Vi prego qualcuno della redazione mi aiuti!!!

Tra tutti gli utenti che sono autorizzati ad accedere a un sistema GNU/Linux facendo il login con il proprio nome utente e relativa password, ve ne è uno molto particolare: root. 'root' è l'amministratore del sistema (ha insomma pieni poteri :) e viene appunto utilizzato esclusivamente per la configurazione del sistema, l'installazione di nuovi programmi, la gestione di determinati servizi etc... Per determinate operazioni è quindi necessario disporre dei privilegi di root, di cui potrete temporaneamente usufruire senza dovervi riautenticare nel sistema ma semplicemente digitando da shell 'su' e quindi la password di root; una volta terminato con 'exit' potrete tornare ad essere utenti normali.

>> Ritorno alla console

La mia distribuzione si avvia direttamente in modalità grafica; è possibile comunque poter lavorare completamente a riga di comando (non in una finestra "terminale" per intenderci)?

Come abbiamo detto in passato, Linux è un sistema multitasking e multiutente; questo significa che più utenti possono lavorare contemporaneamente sulla stessa macchina ed eseguire più programmi insieme. Per poter sfruttare appieno queste potenzialità anche in locale, oltre all'eventuale server grafico, Linux presenta di default sei console virtuali in modalità testo: per passare da una all'altra è sufficiente utilizzare la combinazione di tasti CTRL+ALT+F(1-6) dove l'ultimo tasto è uno dei primi sei tasti funzione, a cui sono associate le sei console. Ovviamente potete autenticarvi come utenti diversi nelle diverse console e, una volta finito, potete tornare ad X-Window utilizzando questa volta F7.

lele - lele@altos.tk

Hacking trough OS X

Non è un caso che uno dei libri più famosi su Mac OS X si chiami "Il manuale mancante". Molti degli aspetti del sistema funzionano in modo diverso da prima, ma diverso anche dai sistemi Unix tradizionali.

È cosa risaputa che l'attuale sistema operativo di Apple abbia un "motore" UNIX, per la precisione una versione di BSD 4.4 chiamata Darwin (http://developer.apple.com/darwin/).
Viene da chiedersi il **perché della nascita di una nuova "variante" di *NIX** (come se non ce ne fossero già abbastanza). Il motivo è che le fondamenta di OSX sono in realtà un mosaico, composto da vari pezzi. Fondamentale è l'apporto dell'esperienza di NeXT (da cui insieme a Steve Jobs provengono anche molti dei progettisti di X), ma a questa bisogna sommare anche l'aggiornamento del Mac OS "classico" così come le nuove aggiunte e adattamenti prese da altre implementazioni di BSD come FreeBSD, NetBSD e OpenBSD.
Il risultato è che **Mac OS X è un sistema pieno di sorprese, non solo per l'utente tipico Macintosh, ma anche per chi viene, ad esempio, da Linux**.
In questo articolo e nel prossimo articolo vedremo le similitudini e differenze presenti su una parte cruciale dell'OS: il filesystem.

>> Ora mi vedi e ora no

Il filesystem di OSX è un esempio lampante dell'ibridazione attuata. Vediamo per esempio **come viene gestita l' "invisibilità" dei file**.
Il primo metodo è quello **tipico dei sistemi UNIX** e cioé usando come prefisso ".", il punto. Questa tecnica viene usata su varie directory e file di configurazione, ad esempio nella root per nascondere le cartelle

```
.DS_Store
.Trashes
.hidden
.vol
```

che, insieme ad altre, sono invisibili al Finder e al comando "ls" nel Terminale. Per "vedere" tutto basta usare il comando ls, da Terminale, usando l'opzione a (all, tutti)

```
ls -a
```

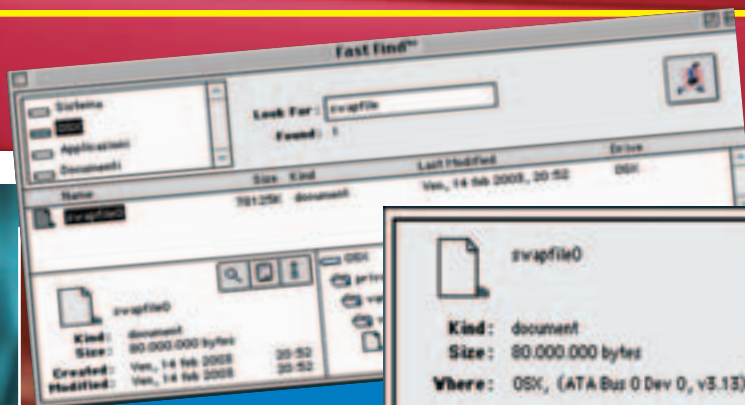
oppure usare una delle numerose utility (come Tinker Tool) che attivano l'opzione nascosta "show all files".
Il secondo metodo è quello **derivato dal vecchio Mac OS e cioé di settare l'attributo "invisible"** con qualche utility, oppure di usare sotto OSX, previa instalalzione dei "developer Tools" di Apple, il comando:

```
SetFile -a V nomefile
```

per riattivare la visualizzazione dal FInder si usa invece

```
SetFile -a v nomefile
```

Il terzo modo si ricollega a uno dei file "svelati" sopra.
Se **.DS_Store** tiene nota delle preferenze relative alla cartella ed ai file contenuti (e riserva alcune sorprese, come vedremo nel prossimo articolo, **.Trashes** contiene i file buttati nel cestino e **.vol/** gli identificativi per ogni documento, lo **.hidden** è uno strumento prezioso, perché non è altro che elenco di file che il Finder deve tenere nascosto.
Non è raro infine che qualche directory o file sia resa invisibile **contemporaneamente in diversi modi**. Un esempio è la directory "/bin" che è sia nell'elenco di ".hidden", e ha anche l'attributo "invisibles" settato. Allo stesso modo bisogna sempre ricordare che se si riavvia con Mac OS 9, **due su tre di questi metodi non funzioneranno e che ci ritroveremo visibili diversi pezzi cruciali del sistema operativo** (come "/mach" ad esempio) con cui è meglio non pasticciare e lasciare dove sono, pena il non funzionamento di X.

Sempre da Mac OS 9 è invece possibile fare altro, ad esempio scoprire che

Riavviando con Mac OS 9, molti dei file e delle cartelle invisibili in X tornano magicamente alla luce.

OSX, come ogni bravo UNIX usa la memoria virtuale e più precisamente una serie di file di memoria virtuale.
I file si trovano in **/private/var/vm/** e sono tutti del peso di cca 76 Mb e numerati progressivamente "swapfile0", "swapfile1" e così via. Ovviamente più ram si ha e meno ce ne ritroveremo.
Per la cronaca è possibile anche, con un po' di smanettamenti, cancellare questi file ma OSX manterrà lo spazio su disco comunque occupato e li ricreerà secondo le esigenze. **L'unico modo per ridurne il numero momentaneamente è un bel riavvio della macchina**.

>> Alias e link

Altro esempio di coniugazione (e coesistenza) di due mondi sono quei file speciali chiamati **collegamenti** su Windows, **alias** su Mac OS e **link** su UNIX.
In OS X ci sono due modi per farli. Il primo è alla vecchia maniera: selezionare un oggetto dal Finder, trascinarlo tenendo premuti i tasti **alt+mela (option+command)**. Al rilascio avremo creato un alias, utilizzabile dai programmi Classic (emulazione), Carbon e Cocoa, ma non da quelli Unix da Terminale.
Per fare contento quest'ultimo, dovremo invece creare un "link" o "symbolic link" (o ancora symlink) usando da Terminale il comando:

```
ln
```

oppure

```
ln -s
```

Il vantaggio di questa tecnica è che oltre ai programmi Unix, i link funzionano anche con tutti gli altri tipi di programmi sunnominati. Attenzione però a non spostare o rinominare il file originale: **i link non funzioneranno, al contrario invece dei vecchi alias**.

>> Altre diversità sostanziali

Oltre a questi "mix", Darwin ha numerose altre peculiarità. Non solo l'ordine e la locazione delle risorse differisce profondamente da Linux o anche dai vari *BSD ma addirittura **la metodologia di interazione con il sistema è spesso diversa**.
Un piccolo intoppo in cui vari utenti sono incappati è che non è possibile modificare il nome dell'hard disk se è avviata la condivisione o che, peggio ancora, il nome dell'hard disk, **se formattato in UFS (Unix File System) è tassativamente "/"**.
Molto più strano è che OS X ha problemi di funzionamento **in presenza di una partizione dal nome "Users"**, che probabilmente da fastidio alla directory dello stesso nome in cui sono i dati dei vari utenti del sistema. Altra originalità è che, di default, **l'utente root è disabilitato ed Apple ne sconsiglia fortemente l'attivazione a tutti coloro che non sono esperti**, suggerendo invece per le funzioni amministrative l'uso a pie' sospinto del comando "sudo", solitamente usato in questo modo

```
sudo nomecomando
```

il tutto seguito dalla password richiesta e che deve essere di un appartenente al gruppo degli amministratori (nessun problema: l'utente principale creato al momento dell'installazione lo è).
I file di configurazione, che hanno estensione .plist, **sono documenti xml, modificabili con comandi da shell o con un PrefEdit**, programma presente nei più volte menzionati Developer Tools (oppure all'url http://www.bresink.de/osx/PrefEdit.html).
Un altra modifica non da poco è che fino alla versione 10.1.X di OSX il programma **NetInfo Manager rimpiazzava alcune funzioni fondamentali di amministrazione come /etc/hosts/" o il sistema di gestione e aggiunta di utenti "/etc/passwd"**.
Fortunatamente con Jaguar (OSX 10.2) NetInfo ha visto cadere il suo ruolo di tool esclusivo ed è ora possibile modificare a mano, o con le numerose utility da shell presenti nei Developer Tools, i vari "etc/group", "/etc/passwd/" (o meglio ancora "/etc/master.passwd", il file shadow che contiene le vere password crittografate).

Gestione NetInfo, o NetInfo manager, è un po' il pannello di amministrazione dell'intero sistema. Ma è meglio non toccarlo se non si sa con precisione cosa si sta facendo.

Nicola D'Agostino
(dagostino@nezmar.com)

COSA SUCCEDE AL

In questa seconda parte dedicata ai protocolli applicativi, analizzeremo altri processi utilizzati quotidianamente da ogni utente.

Hyper-Text Transport protocol, o http, è il cuore del sistema per il trasferimento di ipertesti. Ma cosa si intende per ipertesto? Da cosa è formato e soprattutto… a cosa serve?

Con ipertesto si definisce **un documento che contiene collegamenti (link) ad altri testi, oppure ad altre parti del testo stesso**. Ogni utente che si trova davanti a un qualunque documento di testo si può dire che debba affrontare un “percorso obbligato”, percorso che inizia con l’inizio del documento e termina con la sua fine. La differenza di un ipertesto sta esattamente nell’abolizione di questo obbligo, in quanto **in qualunque punto si possono trovare collegamenti ad altre pagine correlate o a punti diversi della stessa** che, magari, approfondiscono ulteriormente ciò che noi stiamo leggendo. Per semplificare si può affermare che è un po’ come uno di quei libri di avventure dove è il lettore che decide se il Signor X a quell’incrocio deve svoltare a destra oppure a sinistra, decidendo in prima persona il suo “futuro”.

Come risulta ovvio, l’approccio di tipo ipertestuale è tipico e raffrontabile con quello di ogni ricercatore. Mentre un lettore di un giallo inizia dal primo capitolo per arrivare all’ultimo e scoprire l’assassino, un investigatore trae spunti da ogni parola che legge, e da questa parte per effettuare approfondimenti che lo porteranno a smascherare il “maggiordomo”.

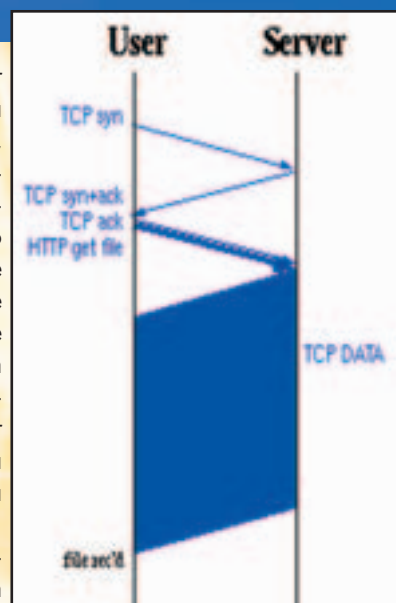
>> La forza della semplicità

Il punto di forza di questo protocollo e la logica su cui si basa la sua creazione è la semplicità. L’http deve essere semplice da utilizzare, semplice da implementare, interscambiabile fra tutte le piattaforme e deve, essenzialmente, essere in grado di trasferire un ipertesto o un file da una macchina ad un’altra impiegando il minor numero di risorse possibili e nel minor tempo raggiungibile.

Si basa essenzialmente su un meccanismo di richiesta — trasferimento.

Risorsa: un servizio oppure un oggetto appartenente alla rete. Le risorse si dividono in due categorie: gli **URL**, acronimo di uniform resource location, che definiscono un “sito”, e gli **URN**, acronimo di uniform resource name, che definiscono un “nome”.

Proprio per questa sua semplicità, il meccanismo di funzionamento è facilmente riassumibile in poche parole: un client, tramite un user agent, invia la richiesta al server, il quale risponde con un messaggio creato con un formato analogo a quello della spedizione. Sia il primo che il secondo messaggio sono di tipo testuale, ma grazie ad una codifica particolare di tipo MIME (Multipurpose Internet Mail Extension) possono contenere al loro interno dei blocchi dati. Tali blocchi sono capaci di trasferire programmi, immagini, testo e quant’altro sia presente sul server.

Il protocollo http è giunto alla **versione 1.1 definita dalla RFC 2068**. Per coloro i quali fossero interessati a dare una scorsa anche alla definizione della versione 1.0 si consiglia la letture della **RFC 1095**.

"DIETRO" BROWSER

User agent: il client si trasforma in user agent non appena inizia ad inoltrare richieste al server. Un esempio tipico di user agent sono i Web browser che noi tutti conosciamo.

>> Analisi del protocollo

In generale un URL del tipo http/1.0 si presenta nel modo seguente:

```
http://host [ ":" porta ]
[percorso_assoluto]
```

Dove **host** descrive l'hostname desiderato, **port** è il punto in cui inserire il numero di porta e **percorso_assoluto** specifica la risorsa richiesta.
Se andiamo, invece, ad analizzare il protocollo http/1.1 vediamo che la rispettiva URL si presenta nel modo seguente:

```
http://host [ ":" port ]
[absolute_path [ "?" query ]]
```

Qualunque cosa sia specificata dopo "?" è un contenuto elaborato da uno script in esecuzione.
Come detto la trasmissione dati inizia con uno scambio di messaggi: questi messaggi possono essere **una richiesta oppure una risposta**. I messaggi possono essere creati secondo due standard, anche se in verità oramai il primo, ovvero quello di tipo **semplice**, è stato quasi del tutto abolito, ed è comunque fortemente sconsigliato. Tanto per dovere di cronaca e per favorire un raffronto, possiamo accennare brevemente alla struttura di questo tipo di messaggi, basati su una richiesta GET a cui il server rispondeva direttamente con la pagina di interesse. Oggi invece con l'introduzione dello standard 1.0 e poi del 1.1, ci troviamo di fronte a **messaggi di tipo complesso**. La richiesta è formata da tre parti essenziali raggruppabili come: **linea di richiesta, intestazione o intestazioni, parte opzionale**. La risposta è anch'essa complessa e strutturata secondo la medesima metodologia: linea di stato, intestazione, parte opzionale. Se vo-

lessimo entrare più nello specifico vediamo che: **la linea di richiesta** è formata da tre elementi separati tra di loro, e più esattamente dal **metodo di richiesta**, definito come get (utilizzato per informazioni sottoforma di entità),

Entità: una risorsa del tipo "dati" oppure una risorsa del tipo "servizio" erogato a seguito di una particolare richiesta.

head (funziona come il comando get, con la differenza che sono restituite solo le metainformazioni) oppure post (spedisce un'entità in modo che venga subordinata all'unità ricevente).

Le intestazioni sono URL oppure URN, **la parte opzionale** quando presente definisce lo standard http uti-

Connessione nel momento in cui il client del computer da cui stiamo navigando si connette ad un server remoto per attingere informazioni da esso.

lizzata, 1.0 oppure 1.1. Questa linea di richiesta termina sempre con un **CRLF** (sequenza di fine riga) **La linea di stato** è identica a quella di richiesta fatto salvo per due piccole varianti: il tipo di http utilizzato è scritto per primo, contiene un codice di ritorno con un significato particolare. Il codice di ritorno è formato da tre cifre, in cui la prima indica il responso ed è fissa, mentre le seconde due cambiano riguardo piccole differenze o motivazioni della risposta stessa; i codici 1xx sono riservati ad usi futuri, 2xx sono di accettazione, 3xx chiedono di effettuare ulteriori operazioni prima di completare la richiesta, 4xx rimanda la richiesta indietro a causa di errori di sintassi, 5xx è un rifiuto per motivi interni al server.
Analizziamo infine **le intestazioni** di ogni messaggio. Sono essenzialmente divisibili in quattro categorie differenti: generali, di entità, specifiche per la richiesta, specifiche per la risposta. Il formato di ogni richiesta è lo stesso, ed è strutturato nel modo seguente: nome di un campo seguito da due punti, da uno spazio, dal valore per quel campo e da una sequenza CRLF di chiusura. Un esempio di intestazione di tipo generale è la data; essa, a seconda dello standard che vogliamo utilizzare, può essere scritta in tre modalità differenti

(per le specifiche tecniche si consigliano gli RFC 822 ed 850).
Le intestazioni specifiche possono contenere dei campi particolari, utili nella definizione di alcune ricerche. Alcuni esempi, riguardo alle richieste, possono essere: **user-agent** (riporta informazioni sul software utilizzato per effettuare la richiesta), **if-modified-since** (condiziona una risposta ad una richiesta in base ad una data ed un'ora), **authorization** (specifica le credenziali di un user-agent per quella connessione).
Riguardo alle intestazioni specifiche per le risposte possiamo avere: **location** (restituisce la locazione precisa di una risorsa), **server** (riporta informazioni sul server al quale ci siamo collegati).

>> Connessioni sicure

Per completezza vogliamo accennare anche al **protocollo https, ovvero http su SSL**. È un protocollo che trova la sua applicazione in quelle pagine in cui il contenuto debba essere cifrato prima di essere inviato al server, come per esempio le transazioni finanziarie, i codici delle carte di credito e altre situazioni analoghe. Se diamo uno sguardo alla RFC2246, possiamo vedere che esistono molti tipi differenti di protocolli SSL, ognuno di quali può poi scegliere fra più standard di crittografia; proprio a causa di questa complessità invitiamo ad analizzare il suddetto RFC in caso di dubbi a riguardo.

>> A che serve tutto ciò?

Ma in tutto ciò la pratica dove sta? Mettiamola così...saper manipolare gli URL può essere l'arma vincente per entrare dentro un sistema e per violare macchine server. Come ovvio non dirò cosa fare e come, ma cercherò di farvi capire che talvolta **un %% piazzato nel punto giusto può aprire un'autostrada che conduce ovunque**.
L'URL è una microapertura che permette di comunicare con strutture anche molto grandi alle sue spalle. Immaginatevi una grande rete di server, protetta da firewall sicurissimi e dai sistemi di sicurezza tecnologicamente più avanzati; nonostante ciò, **magari esiste una pagina web, anche una sola, visibile a chiunque** voglia accedervi per esempio per pubblicizzare i server stessi. Sarà proprio da lì, da quella minuscola apertura, che noi dovremo iniziare a scavare per aprirci una galleria verso l'interno. Tutto ciò, come detto, viene fatto sfruttando gli URL e le modifiche alla loro struttura.
Ma come è fatto questo URL? E' strutturato secondo la seguente struttura:

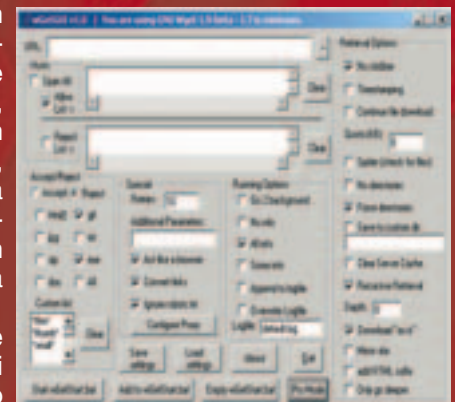
```
protocollo://server/percorso_alla_risorsa?parametri
```

Analizzando un esempio reale possiamo provare con: http://www.ilfibra.it/ef1.htm dove http:// è il protocollo, www.ilfibra.it è il server (server virtuale nel nostro caso), ef1.htm è il percorso per trovare la risorsa desiderata. In questo URL mancano i ?parameters in quanto questa non è un'applicazione con un database alle spalle. Se avessi www.comprami.it/buy.asp?obj=XXXY&payment=paypal allora noterei che obj=XXXY&payment=paypal sono i parametri di cui ha bisogno l'applicazione ASP per concludere e gestire la vendita ed il pagamento dell'oggetto XXXY.

CAT4R4TTA,
cat4r4tta@hackerjournal.it

Come "spremere" il protocollo

Spesso le risorse disponibili su protocollo http possono essere sfruttate in modo più efficace lasciando da parte il browser e usando un'utility a linea di comando come curl o wget (esistono, in effetti, anche varie interfacce grafiche che ne sfruttano le funzionalità, e che vedete in questo riquadro). Curl (http://curl.haxx.se/) gestisce protocolli di vario tipo (http, https, ftp, ftps, gopher, telnet...), sia in download che in upload, e permette di controllare ogni dettaglio della richiesta: oltre all'url, si può anche specificare (e quindi "falsificare") la presenza di un cookie, il tipo di browser o di piattaforma utilizzata, o indicare un indirizzo di provenienza (cioè simulare il clic effettuato su un'altra pagina, dello stesso sito o di un altro). Tanto per fare un esempio, nel gioco Try2Hack (www.try2hack.nl), per superare uno dei livelli bisogna accedere a un pagina partendo da un link del sito microsoft.com, utilizzando Internet Explorer su un sistema Linux, tutte condizioni impossibili da realizzare, ma facili da falsificare con curl.

Per chi ha bisogno di scaricare una lunga serie di file in sequenza, curl permette di specificarli tutti con una sola riga. Per esempio, il comando

```
curl http://www.hackerjournal.it/fuffa/fuffa[01-99].txt -O
```

scaricherà tutti i file da fuffa01.txt a fuffa99.txt e li salverà su disco.

Wget (www.gnu.org/software/wget/wget.html) ha funzionalità analoghe, e la scelta tra uno o l'altro programma è spesso questione di preferenza personale (o di disponibilità per il proprio sistema; curl infatti esiste in forma già compilata per molte più piattaforme).

AVVIO E CHIUSURA AUTOMATICA DEL SERVER WEB APACHE SU LINUX

CONFIGURARE APACHE

Sullo scorso numero abbiamo visto come installare Apache e dargli una configurazione minima. E' tempo di impostare alcune altre opzioni...

Dopo aver installato Apache sul proprio computer, vediamo come farlo partire dopo ogni avvio della macchina. Per poter far partire un processo all'avvio, bisogna innanzitutto conoscere un po' **come funziona il sistema per la gestione dell'avvio e interruzione (kill) dei processi** che forniscono i vari servizi. In questo sistema esistono cinque livelli fondamentali:

livello 0 -> Spegni macchina
livello 1 -> Avvio monoutente
livello 3 -> Avvio multiutente modalità testo
livello 5 -> Avvio multiutente modalità grafica
livello 6 -> Riavvio macchina

Per ogni livello vengono fatti partire o stoppare dei processi. I processi interessati sono degli script di shell e si trovano nella cartella /etc/init.d/

Per ogni livello esiste una directory /etc/rc?.d dove il ? è il numero di livello a cui si fa riferimento (le directory possono cambiare in base alle versioni). In queste cartelle ci sono dei link simbolici agli script nella cartella /etc/init.d/ con questa sintassi:

```
[S/K]NumProcesso
```

Se il nome inizia con S, il processo dovrà essere avviato (Start), mentre se inizia con K dovrà essere fermato (Kill), Num è un numero identificativo del processo, e Processo il nome del file eseguibile.
Dopo questa breve e veloce spiegazione qui seguito riporto come far partire il server web con l'esempio capirete anche come funziona l'avvio di qualsiasi altro processo.

>> Sotto con Apache

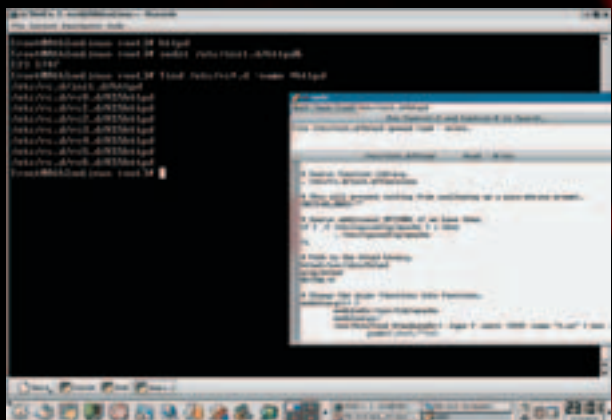
Per iniziare dobbiamo accertarci che esista il file **/etc/init.d/httpd**, lo script che avvierà il nostro servizio di web server. Normalmente è già presente, e in questo caso si dovrà soltanto controllare che tutte le directory che richiama esistano, altrimenti modificarle in modo opportuno (per esempio, se si è cambiata la directory dove sono installate le librerie che httpd utilizza). Se si deve creare un file httpd in init.d, bisogna conoscere la programmazione della shell e, prendendo come riferimento il file script per l'avvio di un altro processo, convertirlo per avviare il file /usr/sbin/httpd/ e salvarlo come /etc/init.d/httpd.
Accertato che esista lo script di cui abbiamo appena parlato, si devono creare tutti i link simbolici in base all'avvio o arresto del sistema per automatizzare il server web. Sfogliando le directory /etc/rc?.d/ noterete che, se precedentemente era stato installato un web server, tutti i collegamenti esisteranno già e avranno un numero identificativo. Annotate questo numero e cancellate questi collegamenti per creare quelli nuovi. Potete cancellare i link col comando rm /etc/rc?.d/K15httpd. Supponendo che il numero del processo sia 15, i link di avvio vanno creati nel seguente modo:

```
ln -s /etc/init.d/httpd
/etc/rc1.d/S15httpd
ln -s /etc/init.d/httpd
/etc/rc3.d/S15httpd
ln -s /etc/init.d/httpd
/etc/rc5.d/S15httpd
```

mentre in fase di spegnimento si dovrà "uccidere" il processo così:

```
ln -s /etc/init.d/httpd
/etc/rc0.d/K15httpd
ln -s /etc/init.d/httpd
/etc/rc6.d/K15httpd
```

Ora il nostro server Web verrà avviato non appena il sistema avrà completato il boot, e andrà a dormire prima di spegnere il computer. Ora che avete un sito Web sul vostro computer, potete divertirvi ad attaccarlo senza fare casino in giro :-)

Per avviare automaticamente Apache, bisogna creare dei link simbolici nelle directory appropriate.

Prima di iniziare conviene vedere se esistono già i file per l'avvio e lo spegnimento del server http.

COME FUNZIONA L'IDENTIFICAZIONE DEL TELEFONO CON SIM E CODICE IMEI

I NUMERI DI TARGA DEL CELLULARE

No, non pensate al furgone con le sirene blu. Stiamo proprio parlando dei telefonini...

Sullo scorso numero abbiamo parlato della funzione di identificazione del chiamante (banalmente, il fatto che quando chiamiamo qualcuno, sul suo visore appare il nostro numero di telefono), di come è possibile disabilitare questa funzione anche nei fissi, e abbiamo accennato al fatto che la disabilitazione funziona solo per gli utenti finali. **Per gli operatori telefonici infatti (e quindi per le forze dell'ordine), non ci sono segreti**. Vediamo esattamente quali dati il nostro cellulare distribuisce in giro, e per cosa possono essere usati.

>> Siamo tutti dei numeri

Sarà una frase fatta, ma è vero. Il numero più ovvio che ci viene associato è il numero di telefono, che dipende SIM dell'operatore telefonico. Avendo fornito **i nostri documenti al momento dell'attivazione**, l'associazione tra noi e il numero è presto fatta (in Svizzera fino a poco tempo fa erano in vendita SIM anonime, ma il tutto è stato bloccato perché venivano utilizzate da – indovinate un po' – niente meno che Al Qaeda).

Il codice che invece molte meno persone conoscono è l'**IMEI (International Mobile station Equipment Identity)**. Si tratta di un numero che identifica in modo univoco il telefono stesso; ogni cellulare ne ha uno, fissato dal produttore. Normalmente è composto da 15 cifre, ed è visibile su un'etichetta sul telefono, la scatola o sui manuali. Con molti cellulari, può essere visualizzato digitando il numero ***#06#**.

>> Registri incrociati

Quando il nostro telefono si collega a una cella del gestore, **gli comunica sia il codice IMEI che il numero di telefono (dati della SIM)**. Se tutto va bene, la cella potrà accettare chiamate dal nostro telefono, e sa che può inviarci una chiamata al numero che le abbiamo comunicato. In alternativa, la cella potrebbe anche rifiutare il collegamento. In alcuni posti per esempio esistono dei registri dei cellulari rubati: si comunica il codice IMEI all'operatore, e da quel momento il cellulare non potrà più essere utilizzato (molto spesso, però, solo sulla rete di quell'operatore).

Vediamo di mettere insieme tutte queste informazioni per capire **cosa l'operatore sa su di noi...**

Innanzi tutto può sapere sempre dove siamo. Ogni cella GSM è abbastanza piccola (nelle grandi città, qualche isolato). In ogni momento, il gestore **sa quindi dove si trova la SIM associata al nostro nome** (ovviamente, se è inserita in un telefono acceso…).

Avendo registrato IMEI e SIM, se con la stessa SIM si collegano due telefoni con IMEI diverso, l'operatore **sa che abbiamo cambiato telefono**. Al contrario, se inseriamo una nuova SIM nel telefono abituale, l'operatore può dedurre che **– anche con una SIM diversa –** siamo sempre noi a effettuare la chiamata (oppure che abbiamo ceduto il telefono a un'altra persona, con una SIM diversa).

Il succo della questione è questo: se avete "per caso trovato" una SIM card, e la usate per fare "scherzi telefonici" dopo averla infilate nel cellulare che usate solitamente con la vostra SIM regolarmente acquistata, sappiate che possono tranquillamente venirvi a prendere. **Fate i bravi...**

COM'È FATTO IL CODICE IMEI

Supponiamo che il codice sia **123456-78-654321-0**

123456 - Le prime sei cifre sono il Type Approval Code (le prime due sono il codice della nazione).

78 - Le due cifre successive sono il Final Approval Code (FAC).

654321 - Le sei cifre seguenti sono il numero di serie del telefono.

0 - L'ultima cifra è un codice di controllo.

IRC E GLI FSERVE

Pensavate che il file sharing fosse nato con Napster? Invece esisteva già sulle reti di chat Irc! E a ben vedere, Napster non era altro che un client Irc taroccato...

Quando si parla di file sharing si pensa subito a programmi come WinMX o Kazaa per la condivisione dei propri file. **Gli fserve sono un'altra forma di file sharing**, poco utilizzata ma altrettanto efficace. Si basano su IRC, la più famosa rete di server per la chat. Gli fserve (il cui nome significa file server) sono un sistema di condivisione di file in IRC e **consistono in utenti con particolari client che permettono agli altri di navigare all'interno delle cartelle condivise**, come si naviga in un FTP, con la possibilità di scaricare i file raggruppati per categorie. Chiunque può installare sul proprio computer un fserve ma è consigliabile soprattutto per chi possiede una linea veloce come l'ADSL per non penalizzare con rallentamenti la propria connessione e i download dei file. Bisogna pensare poi che questo metodo permette agli altri utenti di accedere ai propri file sull'hard disk e per questo **è necessario configurarlo al meglio per non concedere l'accesso a cartelle o file contenenti informazioni riservate.**

>> Come funziona un fserve

Molti di voi avranno già installato sul proprio computer un client per l'accesso ad IRC, come il famoso mIRC; chi non ce l'ha puoi scaricarlo gratuitamente la versione più aggiornata dal sito del produttore www.mirc.com.
Una volta scaricato il file di installazione, generalmente di dimensioni non elevate, basterà installarlo per avere accesso alla chat. **Una delle reti di server su cui maggiormente vengono utilizzati gli fserve è DALnet**, perciò prenderemo questa come esempio. È però possibile attuare lo stesso procedimento su tutte le altre reti.
Appena installato e avviato il mIRC, vi apparirà la schermata delle opzioni in cui vanno inseriti i propri dati (nome ed email non devono essere necessariamente validi, si possono inserire anche dati falsi). Fatto questo si potrebbe personalizzare al meglio il client configurando anche tutte le altre opzioni ma non è fondamentale perciò passiamo oltre.

La finestra dello Status, l'unica ad essere sempre aperta in mIRC, è quella che ci permettere di comunicare col server e leggere le sue risposte, quindi la prima cosa da scriverci è il comando per collegarsi ad un server DALnet. Digitiamo nello Status **/server arcor.de.eu.dal.net** e dopo pochi secondi saremo connessi e pronti a cercare il fileserver che ci interessa.
Tramite il comando **/list <argomento>** è possibile trovare la lista dei canali presenti che trattano un determinato argomento, scrivendo per esempio **/list mp3** ci appariranno tutti i canali che trattano di mp3, ma non tutti dovranno necessariamente contenere fileserver (scrivendo solo **/list** avremo la lista di tutti i canali presenti sul server). Ad esempio con **/list roswell** ci apparirà:

```
#crashdown                   48      Canale
Ufficiale del telefilm Roswell e del sito…
#roswell-episodes           25      English
channel of roswell, the founder said…
#roswell                     18      in 1947 at
roswell something appened…
```

>> Interroghiamo l'fserve

A questo punto entriamo in un canale scrivendo **/join #canale**, in questo caso **/join #crashdown** e visualizziamo la lista degli fserve presenti per vedere cosa offrono scrivendo **!list** nel canale. Apparirà qualcosa del genere:

```
<{RoSwElL}>: (File Servers Online)
Triggers:(!roswell) Snagged:(3.80Gb in 295
files) Min CPS:(0.9Kb/s)    Record
CPS:(56.4Kb/s by toxen) Online:(0/4)
Sends:(0/2) Queues:(0/25) Accessed:(5622
times) Note:(tutti gli episodi della
prima,seconda e terza serie) «~{Polaris
SE}~»
<Nasedo>: (File Servers Online)
Triggers:(!roswell-mp3s & !mp3roswell)
Snagged:(1.16Gb in 378 files) Min
CPS:(0.7Kb/s)    Record CPS:(48.2Kb/s by
toxen) Online:(6/10) Sends:(5/8)
Queues:(0/35) Accessed:(4542 times)
Note:(non sovraccaricatemi) «~{Polaris SE}~»
```

Analizziamo le informazioni più importanti ricevute dal fileserver:

Triggers: è il comando da scrivere in canale per aprire una sessione con un determinato fserve per navigarci e scaricare i file;
Snagged: indica la quantità di materiale contenuto nell'fserve e il numero di file presenti
Sends: indica il numero di persone che stanno scaricando affiancato dal numero massimo di download possibili contemporaneamente;
Queues: indica il numero di persone in attesa per scaricare affiancato dal numero massimo che possono restare in attesa; importante per stabilire quando bisognerà aspettare per il proprio turno.

>> Scaricare i file

Scelto il file server, scriviamo il trigger nella finestra del canale e automaticamente ci apparirà una richiesta di DCC Chat (simile ad una normale query solo che avviene tra due utenti senza passare per il server). Una volta accettata la sessione di chat, si ha l'accesso alle cartelle dell'fserve per navigarci e scaricare i file. È importante ricordare che se un utente rimane nel fileserver senza eseguire alcuna operazione, sarà automaticamente disconnesso dopo 30 secondi.
All'interno del file server ci apparirà un messaggio di benvenuto con le informazioni necessarie all'uso. Per esempio:

```
DCC Chat session
Client: {RoSwElL} (80.117.125.47)
Acknowledging chat request...
DCC Chat connection established
<{RoSwElL}>: Roswell File Server with
Advanced File Serving features.
 <{RoSwElL}>: Insta-Send is currently
Enabled and set for files smaller then
48.8KB.
 <{RoSwElL}>: Anti-Camp is currently On
<{RoSwElL}>: You are visitor number: 936
<{RoSwElL}>: Accepted commands are: cd, ls,
dir, read, get, stats, who, sends, queues,
clr_queues, terms
<{RoSwElL}>: For more info about these com-
mands, type !help.
<{RoSwElL}>: ______________________________
__________
<{RoSwElL}>: By Accepting this File Server
Session you agree to any terms set by this
servers administrator.
<{RoSwElL}>: Type !terms to see what if any
exist.
<{RoSwElL}>: ********************** Top 5
Most Requested **********************
<{RoSwElL}>: [#1]  Ligabue (121)
<{RoSwElL}>: [#2]  Episodi di Roswell  (61)
<{RoSwElL}>: [#3]  Film (13)
<{RoSwElL}>: [#4]  Comici  (4)
<{RoSwElL}>: -
<{RoSwElL}>: Current Queue Status:«0/25»
Your Personal Queue Status:«0/4»
[<{RoSwElL}>: -
<{RoSwElL}>: mIRC v6.02 File Server
<{RoSwElL}>: Use: cd dir ls get read help
exit
<{RoSwElL}>: [\]
```

A questo punto non resta che girare per le varie cartelle e scaricare i file che ci interessano con i comandi che vedremo in seguito, in alcuni casi potrebbe essere necessario aspettare il proprio turno per scaricare quando un fserve è affollato.

{RoSwElL}

COMANDI E OPZIONI

Una volta avuto l'accesso al file server, questo **ci indicherà direttamente i comandi disponibili che possiamo utilizzare**; questi potrebbero variare da un fserve ad un altro ma generalmente sono sempre gli stessi e, pur cambiando il loro nome, la funzione è uguale. Vediamo i principali:

cd <cartella> permette di passare alla directory o cartella specificata.
dir [-b|k] [-#] [/w] visualizza i nomi e la dimensione di ogni file contenuto della directory in cui ci si trova, l'opzione /w forza un elenco più grande, l'opzione [-b|k] permette di visualizzare la dimensione mentre l'opzione [-#] specifica il numero di file su ogni linea.
ls [-b|k] [-#] permette di visualizzare l'elenco dei nomi di ogni file nella directory corrente utilizzando una lista ampia.
get <nomefile> permette di scaricare dal fileserver il file specificato.
read [-numerorighe] <nomefile.txt> permette di leggere un file di testo senza doverlo scaricare; all'utente verranno inviate per default 20 righe e poi verrà chiesto se desidera continuare nella visualizzazione del file o abbandonarla mentre l'opzione -numlines cambia il numero di linee di default da visualizzare con un valore compreso tra 5 e 50.
help visualizza i comandi disponibili per un determinato fileserver.
exit termina la connessione con il fileserver.